Some Exponential Diophantine Equations

by

Automan Sibusiso Mabaso

Thesis presented in partial fulfilment of the requirements for the degree of Master of Science

at

Stellebosch University

Supervisor: Dr. Arnold P Keet

Department of Mathematical Sciences

Faculty of Science

Date: December 2013

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the authorship owner thereof (unless to the extent explicitly otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

_____

AS Mabaso

Date: August 2013

Abstract

The aim of this thesis is to study some methods used in solving exponential Diophantine equations. There is no generic method or algorithm that can be used in solving all Diophantine equations. The main focus for our study will be solving the exponential Diophantine equations using the modular approach and the linear forms in two logarithms approach.

Firstly we will analyse a proof by Alexandru Gica who used the modular approach. He works modulo different numbers to reduce the base and the exponent respectively, to show that $(x, y) = (1, \pm 4)$ are the only solutions of the exponential Diophantine equation $y^2 = 5^x + 11^x$. We show that this method does not work for the equation $y^2 = 5^x + 31^x$.

Lastly we will analyse a proof by Yann Bugeaud who used linear forms in two logarithms to find an upper bound of n in the exponential Diophantine equation $x^2 - 2^m = y^n$. First Yann Bugeaud bounded m using a non archimedean linear form in two logarithms. So we look at some of the theory of p-adic numbers to prepare for this.

Uittreksel

Die doel van hierdie tesis is om sommige metodes te bestudeer om sekere Diophantiese vergelykings op te los. Daar is geen metode wat alle Diophantiese vergelykings kan oplos nie. Die fokus van os studie is hoofsaaklik om eksponensiele Diophantiese vergelykings op te los met die modulêre metode en met die metode van lineêre vorms in twee logaritmes.

Eers analiseer ons 'n bewys van Alexandru Gica wat die modulêre metode toegepas het. Hy het modulo verskeie getalle gewerk om die basis en die eksponent te reduseer om aan te toon dat $(x, y) = (1, \pm 4)$ die enigste oplossings van die eksponensiele Diophantiese vergelyking $y^2 = 5^x + 11^x$ is. Ons toon aan dat hierdie metode nie slaag in die geval van die vergelyking $y^2 = 5^x + 31^x$ nie.

Laastens analiseer ons 'n bewys van Yann Bugeaud wat lineêre vorms in twee logaritmes gebruik het om 'n bogrens vir n in die Diophantiese vergelyking $x^2 - 2^m = y^n$ te bepaal. Hy het eers 'n nie-archimediese lineêre vorm in twee logaritmes gebruik om 'n bogrens vir m te bepaal. Dus kyk ons na 'n gedeelte van die teorie van p-adiese getalle om hiervoor voor te berei.

Dedication

Mother

Acknowledgements

I would like to take this opportunity to thank my supervisor for his unwavering support in my journey towards finishing my thesis. I would also like to thank Prof Barry Green for his encouraging words and secretary for the Department Mathematical Sciences, Mrs LM Adams, for her help when I was stuck with LATEX, scanning and emailing me comments from my supervisor.

Mangithathe futhi lelithuba ukubonga umama wami ohlala njalo engibeka emkhulekweni. Ngithi Mtungwa! Mbhulase! nina ena....!!

Above all I thank the Almighty.

Contents

Chapter 1

Introduction

Diophantine equations get their name from Diophantus of Alexandria. Diophantus was a well know mathematician of the 3rd century. He wrote a highly regarded treatise he called the Arithmetica. The mathematical study of Diophantine problems he initiated is called 'Diophantine Analysis'. The questions in Diophantine analysis we ask about a Diophantine equation include:

- are there any solutions?
- are there finitely or infinitely many solutions?
- can all the solutions be found in theory?

These are some of the questions we will consider when we analyse the Diophantine equations in the next chapters.

A Diophantine equation is an algebraic equation for which integer solutions are sought. An algebraic equation is the one that involves only polynomial expressions in one or more variables. The coefficients of the polynomial should be integers. If a Diophantine equation has variables occurring as exponents, it is called an exponential Diophantine equation.

In the 1950s and 60s, Martin Davis, Julia Robertson and Hilary Putnam showed that an algorithm to determine the solubility of all exponential Diophantine equations is impossi-

ble. Yuri Matiyasevish extended that work in 1970 by showing that there is no algorithm for determining whether an arbitrary Diophantine equation has integral solution(s).

The references for this chapter are [16] and [20].

Chapter 2

The Diophantine equation

$$y^2 = 5^x + 11^x$$

2.1 Introduction

The aim of this chapter is to analyse the modular approach used by ALEXANDRU GICA in [5] in showing that the only solutions of the exponential Diophantine equation $y^2 = 5^x + 11^x$ are $(1, \pm 4)$ and this equation has no solution in the quadratic ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. We will show that this approach used by ALEXANDRU in Theorem 2.6 breaks down towards the end when trying to show that $(1, \pm 6)$ are the only solutions of the exponential Diophantine equation $y^2 = 5^x + 31^x$ and it has no solution in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

The main references for this chapter are [4], [5], [7], [10] and [17].

Before proving Theorem 2.6 we will prove the following:

1. There are no units in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ that lie between 1 and $\frac{1+\sqrt{5}}{2}$.
2. The set of units in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is $\left\{\pm\left(\frac{1+\sqrt{5}}{2}\right)^n \mid n \in \mathbb{Z}\right\}$.

3. $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a UFD.

4. If D is an integral domain and $a, b \in D$. Then $\langle a\rangle = \langle b\rangle$ if and only if $\frac{a}{b} \in U(D)$, where $U(D)$ denotes the set of units in D.

Lemma 2.1 *There is no unit* $\lambda \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ *satisfying* $1 < \lambda < \frac{1+\sqrt{5}}{2}$.

Proof

Suppose on the contrary that there exists such a unit λ. There are two monomorphisms : $\mathbb{Q}(\sqrt{5}) \to \mathbb{C}$, i.e the identity and $x+y\sqrt{5} \mapsto (x+y\sqrt{5})' = x-y\sqrt{5}$, where $x, y \in \mathbb{Q}$. As λ is a unit, then $\lambda u = 1$, for some $u \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, hence $(\lambda u)(\lambda u)' = (\lambda\lambda')(uu') = 1$. But $\lambda\lambda' \in \mathbb{Z}$ and $uu' \in \mathbb{Z}$, so that $\lambda\lambda' = \pm 1$. We consider the two cases $\lambda\lambda' = 1$ and $\lambda\lambda' = -1$.

For $\lambda\lambda' = 1$, $\frac{\sqrt{5}-1}{2} < \lambda' < 1$. Now, $1,6 < \frac{1+\sqrt{5}}{2} < \lambda + \lambda' < \frac{3+\sqrt{5}}{2} < 2,6$. So $\lambda' + \lambda = 2$. Now λ and λ' are the roots of $\lambda^2 - 2\lambda + 1 = 0$ and $\lambda = \lambda' = 1$, a contradiction since $\lambda > 1$.

For $\lambda\lambda' = -1$, $\lambda' = -\frac{1}{\lambda}$. So $0 < \lambda + \lambda' < 1$. This contradicts that $\lambda + \lambda' \in \mathbb{Z}$. ■

Theorem 2.2 *The units in* $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ *are* $\pm\left(\frac{1+\sqrt{5}}{2}\right)^n$, $n \in \mathbb{Z}$.

Proof

Let ε be a unit in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ of norm of -1. Let ε^* be a unit in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ of norm of -1 defined by

$$\begin{aligned} \varepsilon^* &= \varepsilon \text{ if } \varepsilon \geq 1 \\ &= \frac{1}{\varepsilon} \text{ if } 0 < \varepsilon \leq 1 \\ &= -\frac{1}{\varepsilon} \text{ if } -1 < \varepsilon \leq 1 \\ &= -\varepsilon \text{ if } \varepsilon < -1, \end{aligned} \tag{2.1}$$

so that $\varepsilon^* \geq 1$. Since $\frac{1+\sqrt{5}}{2} > 1$ we can find an integer n such that $\left(\frac{1+\sqrt{5}}{2}\right)^n \leq \varepsilon^* < \left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$. Since the unit form a multiplicative group so $\varepsilon^* \left(\frac{1+\sqrt{5}}{2}\right)^{-n}$ is a unit in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ of norm -1 satisfying $1 \leq \varepsilon^* \left(\frac{1+\sqrt{5}}{2}\right)^{-n} < \frac{1+\sqrt{5}}{2}$. By Lemma 2.1 there are no units in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ of norm -1 strictly between 1 and $\frac{1+\sqrt{5}}{2}$. Hence $\varepsilon^* \left(\frac{1+\sqrt{5}}{2}\right)^{-n} = 1$ and so $\varepsilon^* = \left(\frac{1+\sqrt{5}}{2}\right)^n$. Then from equation (2.1) we have $\varepsilon = \pm\left(\frac{1+\sqrt{5}}{2}\right)^n$. ■

Definition 2.3 *Let D be an integral Domain. A mapping $\phi : D \to \mathbb{Z}$ is called Euclidean function on D if it has the following properties:*

(i) $\phi(ab) \geq \phi(a)$ for all $a, b \in D$.

(ii) If $a, b \in D$ with $b \neq 0$, then there exist $q, r \in D$ such that $a = bq + r$ and $\phi(r) \leq \phi(b)$.

Theorem 2.4 *$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a UFD.*

Proof

To prove that $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a UFD, we prove first that $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is Euclidean with Euclidean form $|N(\cdot)|$.

Let $x, y \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Then$|N(xy)| = |N(x)| \cdot |N(y)|$ since the norm is multiplicative. Hence $|N(x)| \cdot |N(y)| > |N(y)|$.

Let us consider the number $\frac{x}{y} \in \mathbb{Q}\left(\frac{1+\sqrt{5}}{2}\right)$, so we may write $\frac{x}{y} = a' + b'\left(\frac{1+\sqrt{5}}{2}\right)$ with $a', b' \in \mathbb{Q}$. Let a and $b \in \mathbb{Z}$ be the best approximation to a' and b' i.e

$$|a' - a| \leq \frac{1}{2}, \quad |b' - b| \leq \frac{1}{2}.$$

Let $x = qy + r$, such that $q = a + b\left(\frac{1+\sqrt{5}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. So $r = \left[(a' - a) + (b' - b)\left(\frac{1+\sqrt{5}}{2}\right)\right](y) \in \mathbb{Q}\left[\frac{1+\sqrt{5}}{2}\right]$. Then we let

$\alpha = a' - a$ and $\beta = b' - b$, hence

$$\begin{aligned}
|N(r)| &= |N\left(\left[(a'-a)+(b'-b)\left(\frac{1+\sqrt{5}}{2}\right)\right]\right)N(y)| \\
&= |N\left[(a'-a)+(b'-b)\left(\frac{1+\sqrt{5}}{2}\right)\right]N(y)| \\
&\leq \left|\left(\alpha+\frac{\beta}{2}\right)^2-\frac{5}{4}\beta^2\right|N(y) \\
&\leq \max\left|\left(\left(\alpha+\frac{\beta}{2}\right)^2;\frac{5}{4}\beta^2\right)\right||N(y)| \\
&\leq \max\left(\frac{9}{16};\frac{5}{16}\right)|N(y)| \\
&< \frac{9}{16}|N(y)| \\
&< |N(y)|\,.
\end{aligned}$$

Then $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is Euclidean, hence UFD. ■

Theorem 2.5 *Let D be an integral domain and $a, b \in D$ such that $a \neq 0$ and $b \neq 0$. Then $\langle a\rangle = \langle b\rangle$ if and only if $\frac{a}{b} \in U(D)$, where $U(D)$ is a set of units in D.*

Proof

If $\frac{a}{b} \in U(D)$, then $a = bu$ for some $u \in U(D)$. Let $x \in \langle a\rangle$. Then $x = ac$ for some $c \in D$. Hence $x = buc$ with $uc \in D$. Thus $x \in \langle b\rangle$. We have shown that $\langle a\rangle \subset \langle b\rangle$.

As $\frac{a}{b} \in U(D)$ and $U(D)$ is a group with respect to multiplication, we have $\frac{b}{a} = (\frac{a}{b})^{-1} \in U(D)$. Then $b = au$ for some $u \in U(D)$. Let $x \in \langle b\rangle$. Then $x = bc$ for some $c \in D$. Hence $x = auc$ with $uc \in D$. Thus $x \in \langle b\rangle$. We find that $\langle b\rangle \subset \langle a\rangle$. Thus $\langle a\rangle = \langle b\rangle$.

Conversely, suppose that $\langle a\rangle = \langle b\rangle$. Then $a = bc$ for some $c \in D$ and $b = ad$ for some $d \in D$. Hence $b = bcd$. As $b \neq 0$ we deduce that $1 = cd$ so that $c \in U(D)$. Thus $\frac{a}{b} \in U(D)$. ■

In proving Theorem 2.6 we will be working in the ring of integers $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ which has

$\left\{\pm\left(\frac{1+\sqrt{5}}{2}\right)^n | n \in \mathbb{Z}\right\}$ as a set of its units. The main steps in proving this theorem are proving that:

1. x is an odd integer, hence it can be written as $x = 2k+1, k \in \mathbb{N}_0$ and $k \equiv 4 \pmod 5$ for $k \geq 1$,
2. the exponents of the units in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ for this equation are multiples of six and
3. the equation $5^x + 11^x = y^2$ has no solution modulo 31 in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ if $k \geq 1$ using the Legendre symbol.

Theorem 2.6 *The only solutions of the Diophantine equation*

$$5^x + 11^x = y^2 \tag{2.2}$$

are $(x, y) = (1, \pm 4)$.

STEP 1: Let us prove that x is odd.
Suppose x is even, say $x = 2k$ for $k \in \mathbb{N}_0$. Then $5^x = 5^{2k} \equiv 1 \pmod 4$ and $11^x = 11^{2k} \equiv 1 \pmod 4$, so $5^x + 11^x \equiv 2 \pmod 4$. But $y^2 \equiv 0, 1 \pmod 4$. We have a contradiction, hence x is odd, say $x = 2k+1$ for $k \in \mathbb{N}_0$. ■

Factorising $y^2 - 5^{2k+1} = 11^{2k+1}$ in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ yields $(y + 5^k\sqrt{5})(y - 5^k\sqrt{5}) = 11^{2k+1} = (4+\sqrt{5})^{2k+1}(4-\sqrt{5})^{2k+1}$. Hence $N(y + 5^k\sqrt{5}) = (4+\sqrt{5})^{2k+1}(4-\sqrt{5})^{2k+1}$.

STEP 2: $4 + \sqrt{5}$ and $4 - \sqrt{5}$ are not associates in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Proof

If they are associates then $\frac{4+\sqrt{5}}{4-\sqrt{5}} \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and is a unit in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. But

$$\begin{aligned}\frac{4+\sqrt{5}}{4-\sqrt{5}} &= \frac{(4+\sqrt{5})^2}{11} \\ &= \frac{21}{11}+\frac{8\sqrt{5}}{11} \\ &= \frac{13}{11}+\frac{16}{11}\left(\frac{1+\sqrt{5}}{2}\right) \notin \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]\end{aligned}$$

since $\frac{13}{11}, \frac{16}{11} \notin \mathbb{Z}$. ■

STEP 3: The ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is a UFD, by Theorem 2.4.

STEP 4: $4+\sqrt{5}$ and $4-\sqrt{5}$ are prime in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ since $N(4\pm\sqrt{5}) = 11$ is a prime number. ■

STEP 5: We claim that not both $4+\sqrt{5}$ and $4-\sqrt{5}$ divide $y+5^k\sqrt{5}$ in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Proof

Suppose $4+\sqrt{5}$ and $4-\sqrt{5}$ both divide $y+5^k\sqrt{5}$ in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Since $(4+\sqrt{5})(4-\sqrt{5}) = 11$, then $11 \mid y+5^k\sqrt{5}$

$\Rightarrow \quad y+5^k\sqrt{5} = 11\left(a+b\left(\frac{1+\sqrt{5}}{2}\right)\right), \quad a,b \in \mathbb{Z}$

$\Rightarrow \quad 2y+2\cdot 5^k\sqrt{5} = 11\left((2a+b)+b\sqrt{5}\right)$

$\Rightarrow \quad 2\cdot 5^k \equiv 0 \pmod{11}$.

This is impossible. ■

$4\pm\sqrt{5} > 0$. We assume $y > 0$, then $y+5^k\sqrt{5} > 0$. Using Theorem 2.5 the only possibilities are

$$y+5^k\sqrt{5} = (4+\sqrt{5})^{2k+1}\left(\frac{1+\sqrt{5}}{2}\right)^{m_1}, \quad m_1 \in \mathbb{Z} \tag{2.3}$$

or

$$y + 5^k\sqrt{5} = (4 - \sqrt{5})^{2k+1}\left(\frac{1+\sqrt{5}}{2}\right)^{m_1}, \quad m_1 \in \mathbb{Z}. \tag{2.4}$$

STEP 6: We claim that m_1 is even.

Proof

By equation (2.3) or (2.4)

$$N(y + 5^k\sqrt{5}) = y^2 - 5^{2k+1} = 11^{2k+1}(-1)^{m_1}$$

and to get the original equation, m_1 must be even. ■

Let $m_1 = 2m_2$, where $m_2 \in \mathbb{Z}$. Now $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$ and equations (2.3) and (2.4) become

$$y + 5^k\sqrt{5} = (4 + \sqrt{5})^{2k+1}\left(\frac{3+\sqrt{5}}{2}\right)^{m_2} \tag{2.5}$$

and

$$y + 5^k\sqrt{5} = (4 - \sqrt{5})^{2k+1}\left(\frac{3+\sqrt{5}}{2}\right)^{m_2} \tag{2.6}$$

respectively.

STEP 7: We claim that m_2 is a multiple of 3.

Proof

Let $m_2 = 3m_3 + r$, where $m_3 \in \mathbb{Z}$ and $r \in \{0, 1, 2\}$. But $\left(\frac{3+\sqrt{5}}{2}\right)^3 = 9 + 4\sqrt{5}$. For $r = 1$ equations (2.5) and (2.6) become

$$y + 5^k\sqrt{5} = (4 + \sqrt{5})^{2k+1}(9 + 4\sqrt{5})^{m_3} \cdot \frac{3+\sqrt{5}}{2} \tag{2.7}$$

and

$$y + 5^k\sqrt{5} = (4 - \sqrt{5})^{2k+1}(9 + 4\sqrt{5})^{m_3} \cdot \frac{3+\sqrt{5}}{2} \tag{2.8}$$

respectively. It follows from equation (2.7) that
$2y + 2 \cdot 5^k\sqrt{5} = (4-\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3} \cdot (3+\sqrt{5})$, so $2y + 2 \cdot 5^k\sqrt{5} \equiv 1 + \sqrt{5} \pmod 2$
and then $2y \equiv 1 \pmod 2$, which is not true.
In the same manner, we conclude that it is not possible to have $r = 1$ in equation (2.6).

For $r = 2$, $\left(\frac{3+\sqrt{5}}{2}\right)^2 = \frac{7+3\sqrt{5}}{2}$, equation (2.5) becomes:

$$y + 5^k\sqrt{5} = (4+\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3}\left(\frac{7+3\sqrt{5}}{2}\right), \quad m_3 \in \mathbb{Z}. \tag{2.9}$$

Hence $2y + 2 \cdot 5^k\sqrt{5} \equiv 1 + \sqrt{5} \pmod 2$, so $2y \equiv 1 \pmod 2$ which is not true.

In the same manner it is not possible to have $r = 2$ in equation (2.6). We are now left with $r = 0$.
If $r = 0$, equations (2.5) and (2.6) become

$$y + 5^k\sqrt{5} = (4+\sqrt{5})^{2k+1} \cdot (9+4\sqrt{5})^{m_3}, \quad m_3 \in \mathbb{Z} \tag{2.10}$$

and

$$y + 5^k\sqrt{5} = (4-\sqrt{5})^{2k+1} \cdot (9+4\sqrt{5})^{m_3}, \quad m_3 \in \mathbb{Z} \tag{2.11}$$

respectively. ■

If equation (2.11) holds, then working (mod 4) yields

$$y + 5^k\sqrt{5} \equiv (-\sqrt{5})^{2k+1} \equiv -5^k\sqrt{5} \equiv -\sqrt{5} \pmod 4.$$

Hence $5^k \equiv -1 \pmod 4$, which is not true. We are now left with equation (2.10) to analyse.

STEP 8: We first show that $m_3 \leq 0$.
Suppose $m_3 \geq 1$. We show that this is impossible by comparing the coefficients of $\sqrt{5}$ on the LHS and RHS of the equation $y + 5^k\sqrt{5} = (4+\sqrt{5})^{2k+1} \cdot (9+4\sqrt{5})^{m_3}$ for $m_3 > 0$. Expanding the RHS of this equation, all the coefficients of $\sqrt{5}$ are positive and one of the

terms in $\sqrt{5}$ is $(\sqrt{5})^{2k} \cdot \sqrt{5} \cdot 9^{m_3}$, so $5^k \geq 5^k \cdot 9^{m_3}$ which is not true for $m_3 > 0$. This proves that $m_3 \leq 0$.

STEP 9: We now prove that $m = -(2k+1) + 5n$, for $n \in \mathbb{Z}$. Let us suppose that $k \geq 1$. We have proved in STEP 8 that $m_3 \leq 0$, say $m_3 = -m$, where m is a non negative integer. Then equation (2.10) becomes

$$y + 5^k\sqrt{5} = (4+\sqrt{5})^{2k+1} \cdot (9 - 4\sqrt{5})^m. \tag{2.12}$$

But

$$\begin{aligned}
(9-4\sqrt{5})^m &= \sum_{t=0}^{m} \binom{m}{t} 9^{m-t} \cdot (-1)^t \cdot (4\sqrt{5})^t \\
\left(-1+\sqrt{5}\right)^m &\equiv \binom{m}{0} 9^m - \binom{m}{1} 9^{m-1} \cdot 4\sqrt{5} \,(\text{mod } 5), \text{ if } t \geq 2 \\
&\equiv (-1)^m - m \cdot (-1)^m \sqrt{5} \,(\text{mod } 5)
\end{aligned}$$

and

$$\begin{aligned}
(4+\sqrt{5})^{(2k+1)} &= \sum_{t=0}^{2k+1} \binom{2k+1}{t} 4^{2k+1-t} \cdot (\sqrt{5})^t \\
\left(-1+\sqrt{5}\right)^{(2k+1)} &\equiv \binom{2k+1}{0} 4^{2k+1} + \binom{2k+1}{1} 4^{2k} \cdot \sqrt{5} \,(\text{mod } 5), \text{ if } t \geq 2 \\
&\equiv (-1) + (2k+1)\sqrt{5} \,(\text{mod } 5).
\end{aligned}$$

Then using equation (2.12) and the above congruences and comparing the coefficients of $\sqrt{5}$ on both sides of the equation, we get $5^k \equiv 0 \equiv (-1)^m \cdot (2k+1) - m \cdot (-1)^{m+1} (\text{mod } 5)$. Hence $(2k+1) + m \equiv 0 \,(\text{mod } 5)$. This proves that $m = -(2k+1) + 5n$, for $n \in \mathbb{Z}$ and $k \geq 1$. ■

Now if $m = -(2k+1) + 5n$ we have

$$\begin{aligned}
(9-4\sqrt{5})^m &= (9-4\sqrt{5})^{-(2k+1)+5n} \\
&= \left(\frac{1}{9-4\sqrt{5}}\right)^{2k+1} (9-4\sqrt{5})^{5n} \\
&= (9+4\sqrt{5})^{2k+1} (9-4\sqrt{5})^{5n}
\end{aligned}$$

and equation (2.10) becomes

$$\begin{aligned} y + 5^k\sqrt{5} &= [(4+\sqrt{5})(9+4\sqrt{5})]^{2k+1}(9-4\sqrt{5})^{5n} \\ &= (56+25\sqrt{5})^{2k+1}(9-4\sqrt{5})^{5n}. \end{aligned}$$

STEP 10: We now prove that for $\eta = 56+25\sqrt{5}$, which is $\eta \equiv 1+3\sqrt{5}\,(\text{mod } 11)$, then $\eta^{10k+i} \equiv \eta^i \,(\text{mod } 11)$.

To reduce our equation we do the following calculations modulo 11 in $\mathbb{Z}[\sqrt{5}]$. Note that

$$\begin{aligned} \mathbb{Z}\left[\sqrt{5}\right]/11 &\cong \left(\mathbb{Z}[X]/\left(X^2-5\right)\right)/11 \\ &\cong (\mathbb{Z}/11)[X]/\left(X^2-5\right) \\ &\cong (\mathbb{Z}/11)[X]/(X-4)(X+4) \\ &\cong [(\mathbb{Z}/11)[X]/(X-4)] \oplus [(\mathbb{Z}/11)[X]/(X+4)] \text{ (Chinese Remainder Theorem)} \\ &\cong \mathbb{F}_{11} \oplus \mathbb{F}_{11}. \end{aligned}$$

Since $\sqrt{5}\,(\text{mod } 11) \mapsto (4,-4) \in \mathbb{F}_{11} \oplus \mathbb{F}_{11}$, we have
$\eta \equiv 1+3\sqrt{5}(\text{mod } 11) \mapsto (1+3\cdot 4, 1-3\cdot 4) = (2,0)$. Since the $\gcd(2,11) = 1$, we have $2^{10} = 1\,(\text{mod } 11)$. Then $\eta^{10k+i} \equiv (\eta^{10})^k \cdot \eta^i \equiv (1,0)\eta^i \equiv \eta^i\,(\text{mod } 11)$, for $i \in \mathbb{Z}$. ■

STEP 11: We prove that $k \equiv 4(\text{mod } 5)$ using the equation $y + 5^k\sqrt{5} \equiv \eta^{2k+1}(\text{mod } 11)$ and substitute by the given value of k and compare the coefficients of $\sqrt{5}$ on both sides of the equation. We use the facts that $5^5 \equiv 1(\text{mod } 11)$ and we have from STEP 10 $\eta^{10n} \equiv 1(\text{mod } 11)$ for $n \in \mathbb{N}$.

If $k \equiv 0\,(\text{mod } 5) \Rightarrow k = 5n$ and $2k+1 = 10n+1$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta \equiv 1+3\sqrt{5}\,(\text{mod } 11)$$

gives $5^k \equiv 5^{5n} \equiv 1 \equiv 3\,(\text{mod } 11)$. This is not true.

If $k \equiv 1\,(\text{mod } 5) \Rightarrow k = 5n+1$ and $2k+1 = 10n+3$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^3 \equiv 4+\sqrt{5}\,(\text{mod } 11)$$

gives $5^k \equiv 5^{5n+1} \equiv 5 \equiv 1\,(\text{mod } 11)$. This is not true.

If $k \equiv 2 \pmod 5 \Rightarrow k = 5n + 2$ and $2k + 1 = 10n + 5$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^5 \equiv 5 + 4\sqrt{5} \pmod{11}$$

gives $5^k \equiv 5^{5n+2} \equiv 5^2 \equiv 3 \equiv 4 \pmod{11}$. This is not true.

If $k \equiv 3 \pmod 5 \Rightarrow k = 5n + 3$ and $2k + 1 = 10n + 7$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^7 \equiv -2 + 5\sqrt{5} \pmod{11}$$

gives $5^k \equiv 5^{5n+3} \equiv 5^3 \equiv 4 \equiv 5 \pmod{11}$. This is not true.

If $k \equiv 4 \pmod 5 \Rightarrow k = 5n + 4$ and $2k + 1 = 10n + 9$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^9 \equiv 3 - 2\sqrt{5} \pmod{11}$$

gives $5^k \equiv 5^{5n+4} \equiv 5^4 \equiv -2 \equiv -2 \pmod{11}$. This is true. ■

STEP 12: CONCLUSION

For $k \equiv 4 \pmod 5 \Rightarrow k = 4 + 5n$ and then $x = 9 + 10n$ for some $n \in \mathbb{N}$. For some odd prime p we have $a^{p-1} \equiv 1 \pmod p$ if $\gcd(a, p) = 1$. Let us look for a prime p such that $p - 1$ is a multiple of 10 and $\gcd(5, 11, p) = 1$. The first one which satisfies this condition is $p = 31$, hence $p - 1 = 30$. Since we are working in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, we will take $a = 5$. Hence we will use (mod 30) in reducing exponents and (mod 31) in reducing the bases in the equation $y^2 = 5^x + 11^x$.

Since $x = 9 + 10n$, we have three possibilities (mod 30) i.e $x \equiv 9, 19, 29 \pmod{30}$. We use the fact that $5^3 \equiv 1 \pmod{31}$ and $11^3 \equiv -2 \pmod{31}$. Now let us substitute in the equation $y^2 = 5^x + 11^x$ to test these three cases.

1. If $x \equiv 9 \pmod{30}$, then $y^2 \equiv 1 - 8 \equiv -7 \pmod{31}$. We now show that this is impossible.
   $\left(\frac{-7}{31}\right) = \left(\frac{-1}{31}\right) \cdot \left(\frac{7}{31}\right)$ and $\left(\frac{-1}{31}\right) = -1$, since $31 \equiv 3 \pmod 4$ and $\left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right)$, since $7 \equiv 31 \equiv 3 (\text{mod } 4)$ and hence $\left(\frac{3}{7}\right) = -1$, then $\left(\frac{7}{31}\right) = 1$. Therefore $\left(\frac{-7}{31}\right) = -1$. This shows that -7 is not a quadratic residue mod 31 .

2. If $x \equiv 19 \pmod{30}$, then $y^2 \equiv 5 + 22 \equiv 27 \pmod{31}$. This is impossible since $\left(\frac{27}{31}\right) = \left(\frac{3}{31}\right).\left(\frac{9}{31}\right) = -1$, since $\left(\frac{9}{31}\right) = 1$ and $\left(\frac{3}{31}\right) = -1$.

3. If $x \equiv 29 \pmod{30}$, then $y^2 \equiv 5^2 + 17 \equiv 11 \pmod{31}$. This is impossible since $\left(\frac{11}{31}\right) = -\left(\frac{31}{11}\right) = -\left(\frac{9}{11}\right) = -1$.
This shows that the equation $y^2 = 5^x + 11^x$ has no solution (mod 31) in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ for $k \geq 1$, i.e $x \geq 3$.

Lastly we consider $k = 0$, then we have $x = 1$ and hence $y^2 = 16$ and this implies that $y = \pm 4$. Therefore, we have proved that the only solutions of the Diophantine equation $y^2 = 5^x + 11^x$ are $(x, y) = (1, \pm 4)$. ■

2.2 An Analysis of the Diophantine Equation $y^2 = 5^x + 31^x$ Using the Modular Approach as in Theorem 2.6

We apply the approach used in proving Theorem 2.6 in analysing the equation $y^2 = 5^x + 31^x$ in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and try to show that $(1; \pm 6)$ are the only integer solutions for this Diophantine equation.

Note: The numbering of steps in this proof may not appear in the same sequence as in the proof of Theorem 2.6 as I have left out some common proofs as we are working in the same ring, $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

1. **STEP 1:** We claim that x is odd.

   Proof

   Suppose x is even, let $x = 2k$ for $k \in \mathbb{N}_0$.

$$\begin{aligned} 5 \equiv 1 \pmod{4} \quad &\Rightarrow \quad 5^{2k} \equiv 1 \pmod{4} \\ 31 \equiv -1 \pmod{4} \quad &\Rightarrow \quad 31^{2k} \equiv 1 \pmod{4}. \end{aligned}$$

Then $y^2 = 5^x + 31^x = 5^{2k} + 31^{2k} \equiv 2 \pmod 4$. This is impossible since $y^2 \equiv 0,\ 1 \pmod 4$. ■

$$N\left(\frac{a+b\sqrt{5}}{2}\right) = \frac{a^2-5b^2}{4}, \quad \text{where} \quad a,b \in \mathbb{Z} \quad \text{and} \quad a \equiv b \bmod 2$$

Let $x = 2k+1,\ k \in \mathbb{N}_0$. Hence $5^x + 31^x = 5^{2k+1} + 31^{2k+1} = y^2$

$\Rightarrow \qquad y^2 - 5^{2k+1} = 31^{2k+1}$. But $31 = (6+\sqrt{5})(6-\sqrt{5})$ in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Hence $\qquad (y+5^k\sqrt{5})(y-5^k\sqrt{5}) = [(6+\sqrt{5})(6-\sqrt{5})]^{2k+1} = 31^{2k+1}$. Then

$N(y+5^k\sqrt{5}) = 31^{2k+1}$. But $31 = (6+\sqrt{5})(6-\sqrt{5})$ in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

STEP 2: $6+\sqrt{5}$ and $6-\sqrt{5}$ are not associate in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Proof

$$\begin{aligned}\frac{6+\sqrt{5}}{6-\sqrt{5}} &= \frac{41+12\sqrt{5}}{31} \\ &= \frac{29}{31} + \frac{24}{31}\left(\frac{1+\sqrt{5}}{2}\right) \text{ but } \frac{29}{31}, \frac{24}{31} \notin \mathbb{Z}.\end{aligned}$$

So $\frac{6+\sqrt{5}}{6-\sqrt{5}} \notin \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and hence not a unit in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Hence $6+\sqrt{5}$ and $6-\sqrt{5}$ are not associate. ■

STEP 3: $6+\sqrt{5}$ and $6-\sqrt{5}$ are prime.

Proof

$N(6 \pm \sqrt{5}) = 31$ and 31 is prime. Hence $6+\sqrt{5}$ and $6-\sqrt{5}$ are prime in $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. ■

STEP 4: Either $6+\sqrt{5}$ or $6-\sqrt{5}$ divides $y+5^k\sqrt{5}$, but not both.

Proof

Suppose $6+\sqrt{5} \mid y+5^k\sqrt{5}$ and $6-\sqrt{5} \mid y+5^k\sqrt{5}$. Then $31 \mid y+5^k\sqrt{5}$ and hence $y+5^k\sqrt{5} = 31\left(\frac{a+b\sqrt{5}}{2}\right) \quad a,b \in \mathbb{Z} \quad a \equiv b \pmod 2$, hence $2y + 2\cdot 5^k\sqrt{5} = 31a + 31b\sqrt{5}$.

By comparing coefficient of $\sqrt{5}$ we have $2\cdot 5^k = 31b$ and hence $b = \frac{2\cdot 5^k}{31} \notin \mathbb{Z}$, since $31 \nmid 2$ and $31 \nmid 5^k$. Hence we have proved that it is not possible to have both $6+\sqrt{5}$ and $6-\sqrt{5}$ divide $y+5^k\sqrt{5}$. ■

We have already proved that the set of units in

$$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \quad \text{is} \quad \left\{\pm\left(\frac{1+\sqrt{5}}{2}\right)^n \mid n \in \mathbb{Z}\right\}.$$

Assume $y > 0$, it follows that $y + 5^k\sqrt{5} > 0$. Then using Theorem 2.5 we get:

$$y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}\left(\frac{1+\sqrt{5}}{2}\right)^{m_1}, \quad m_1 \in \mathbb{Z} \tag{2.13}$$

or

$$y + 5^k\sqrt{5} = (6-\sqrt{5})^{2k+1}\left(\frac{1+\sqrt{5}}{2}\right)^{m_1}, \ m_1 \in \mathbb{Z}. \tag{2.14}$$

STEP 5: We claim that m_1 is even.

Proof

From equations (2.13) or (2.14) we have $N(y+5^k\sqrt{5}) = 31^{2k+1}(-1)^{m_1} = y^2 - 5^{2k+1}$ and hence m_1 should be even to get the original equation, say $m_1 = 2m_2,\ m_2 \in \mathbb{N}$. ■

But $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$, so equations (2.13) and (2.14) become

$$y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}\left(\frac{3+\sqrt{5}}{2}\right)^{m_2} \tag{2.15}$$

and

$$y + 5^k\sqrt{5} = (6-\sqrt{5})^{2k+1}\left(\frac{3+\sqrt{5}}{2}\right)^{m_2} \tag{2.16}$$

respectively.

STEP 6: We now prove that m_2 is a multiple of 3.

Let $m_2 = 3m_3 + r$, where $r \in \{0, 1, 2\},\ m_3 \in \mathbb{Z}$.

For $r = 1$, equation (2.15) becomes

$$y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3}\left(\frac{3+\sqrt{5}}{2}\right). \tag{2.17}$$

From equation (2.17) we have $2y + 2\cdot 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3}(3+\sqrt{5})$ and $2y + 5^k\sqrt{5} \equiv (1+\sqrt{5})(\text{mod } 2)$. This implies that $2y \equiv 1\,(\text{mod } 2)$, which is not true.

For $r = 2$, equation (2.15) becomes:

$$y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3}\left(\frac{7+3\sqrt{5}}{2}\right). \tag{2.18}$$

Then $2y + \sqrt{5} \equiv (1+\sqrt{5})\,(\text{mod } 2)$, which is impossible.

Similarly equation (2.17) is not true for $r = 1$ and $r = 2$.

For $r = 0$ equation (2.15) becomes:

$$y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3} \tag{2.19}$$

and equation (2.16) becomes:

$$y + 5^k\sqrt{5} = (6-\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3}. \tag{2.20}$$

If equation (2.20) holds, then $y + 5^k\sqrt{5} \equiv (2-\sqrt{5})\,(\text{mod } 4)$, since $(6-\sqrt{5})^2 \equiv 1\ (\text{mod } 4)$. Hence $5^k \equiv -1\ (\text{mod } 4)$, which is impossible. If equation (2.19) holds, then

$$y + 5^k\sqrt{5} \equiv (2+\sqrt{5})\,(\text{mod } 4), \quad \text{since} \quad (6+\sqrt{5})^2 \equiv 1\ (\text{mod } 4).$$

Hence $5^k \equiv 1\ (\text{mod } 4)$, which is true. So we have to analyse equation (2.19). ■

STEP 7: We claim that $m_3 \leq 0$.

Proof

Suppose $m_3 \geq 1$. From the equation $y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}(9+4\sqrt{5})^{m_3}, m_3 > 0$, expanding the RHS, all the coefficients of $\sqrt{5}$ are greater than zero and one term in $\sqrt{5}$ is $(\sqrt{5})^{2k} \cdot \sqrt{5} \cdot 9^{m_3}$. So $5^k \leq 5^k \cdot 9^{m_3}$ which is not true for $m_3 > 0$. Therefore $m_3 = -m$, where m is a non negative integer. ■

STEP 8: We prove that $m = 2k + 1 + 5n$ for $n \in \mathbb{Z}$. Let us suppose that $k \geq 1$. Substituting by $m_3 = -m$ in equation (2.19) yields

$$y + 5^k\sqrt{5} = (6+\sqrt{5})^{2k+1}(9-4\sqrt{5})^m. \tag{2.21}$$

Expanding the factors on the RHS of equation (2.21) modulo 5 yields:

$$\begin{aligned}\left(1+\sqrt{5}\right)^{2k+1} \equiv (6+\sqrt{5})^{(2k+1)} &= \sum_{t=0}^{2k+1}\binom{2k+1}{t}6^{2k+1-t}\cdot(\sqrt{5})^t \\ &\equiv \binom{2k+1}{0}6^{2k+1} + \binom{2k+1}{1}6^{2k}\cdot\sqrt{5}\,(\text{mod } 5), \text{ if } t \geq 2 \\ &\equiv 1 + (2k+1)\sqrt{5}\ (\text{mod } \ 5).\end{aligned}$$

For the expansion of $(9-4\sqrt{5})^m$ refer to STEP 9 in the analysis of the equation $y^2 = 5^x + 11^x$. Then from equation (2.21) we have $5^k \equiv 0 \equiv (-1)^m \cdot (2k+1) + m \cdot (-1)^m (\text{mod } \ 5)$. Hence $(2k+1)+m \equiv 0 (\text{mod } \ 5)$. This proves that $m = (2k+1)+5n$, for $n \in \mathbb{Z}$ and $k \geq 1$. ■

Now from equation (2.21) we have

$$\begin{aligned}y + 5^k\sqrt{5} &= (6+\sqrt{5})^{2k+1}(9-4\sqrt{5})^{2k+1}(9-4\sqrt{5})^{5n} \\ &= [(6+\sqrt{5})(9-4\sqrt{5}]^{2k+1}(9-4\sqrt{5})^{5n} \\ &= (34-15\sqrt{5})^{2k+1}(9-4\sqrt{5})^{5n}.\end{aligned}$$

Let $\eta = 34 - 15\sqrt{5}$, then $\eta \equiv 1 - 4\sqrt{5}\,(\text{mod } 11)$.

STEP 9: We prove that for $\eta = 34 - 15\sqrt{5}$, $\eta^{10k+i} \equiv \eta^i\,(\text{mod } 11)$.
We have proved in Theorem 2.6 STEP 10 that if $\sqrt{5}\,(\text{mod } 11) \mapsto (4, -4) \in \mathbb{F}_{11} \oplus \mathbb{F}_{11}$.

Now $\eta = 1 - 4\sqrt{5} \pmod{11} \mapsto (1 - 4 \cdot 4)(1 - 4 \cdot -4) = (7, 6)$ and $7^{10} \equiv 1 \pmod{11}$ and also $6^{10} \equiv 1 \pmod{11}$ since the $\gcd(7, 11) = 1$ and $\gcd(6, 11) = 1$. Hence $\eta^{10k} \equiv 1 \pmod{11}$ and $\eta^{10k+i} \equiv \eta^i \pmod{11}$. ■

STEP 10: We prove that $k \equiv 4 \pmod{5}$.
Let us use the fact that $(9 - 4\sqrt{5})^5 \equiv 1 \pmod{11}$, $\eta^{10k} \equiv 1 \pmod{11}$ and $5^5 \equiv 1 \pmod{11}$. From equation (2.21) we have $y + 5^k\sqrt{5} \equiv \eta^{2k+1} \pmod{11}$. In the following steps we will substitute by the given value of k and then compare the coefficients of $\sqrt{5}$ on both sides of this equation.
If $k \equiv 0 \pmod{5} \Rightarrow k = 5n$ and $2k + 1 = 10n + 1$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^{2k+1} \equiv \eta^{10n+1} \equiv \eta \equiv 1 - 4\sqrt{5} \pmod{11}$$

gives $5^k = 5^{5n} \equiv 1 \equiv -4 \pmod{11}$. This is not true.
If $k \equiv 1 \pmod{5} \Rightarrow k = 5n + 1$ and $2k + 1 = 10n + 3$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^{2k+1} \equiv \eta^{10n+3} \equiv \eta^3 \equiv -1 - 2\sqrt{5} \pmod{11}$$

gives $5^k = 5^{5n+1} \equiv 5 \equiv -2 \pmod{11}$. This is not true.
If $k \equiv 2 \pmod{5} \Rightarrow k = 5n + 2$ and $2k + 1 = 10n + 5$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^{2k+1} \equiv \eta^{10n+5} \equiv \eta^5 \equiv -1\sqrt{5} \pmod{11}$$

gives $5^k = 5^{5n+2} \equiv 5^2 \equiv 3 \equiv 0 \pmod{11}$. This is not true.
If $k \equiv 3 \pmod{5} \Rightarrow k = 5n + 3$ and $2k + 1 = 10n + 7$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^{2k+1} \equiv \eta^{10n+7} \equiv \eta^7 \equiv -4 - 3\sqrt{5} \pmod{11}$$

gives $5^k = 5^{5n+3} \equiv 5^3 \equiv 4 \equiv -3 \pmod{11}$. This is not true.
If $k \equiv 4 \pmod{5} \Rightarrow k = 5n + 4$ and $2k + 1 = 10n + 9$ for some $n \in \mathbb{N}$, then

$$y + 5^k\sqrt{5} \equiv \eta^{2k+1} \equiv \eta^{10n+9} \equiv \eta^9 \equiv -1 - 2\sqrt{5} \pmod{11}$$

gives $5^k = 5^{5n+4} \equiv 5^4 \equiv -2 \equiv -2 \pmod{11}$. This is true. ■

STEP 11: If $k \equiv 4 \bmod 5$, then $k = 5n + 4$ for some $n \in \mathbb{N}$ and

$$x = 2k + 1 = 9 + 10n. \tag{2.22}$$

We now look for a prime p greater than 31 such that $p - 1$ is a multiple of 10 and $\gcd(5, 31, p) = 1$. The first one which satisfies this condition is $p = 41$, hence $p - 1 = 40$. Since $\gcd(5, 41) = 1$, then $5^{40} \equiv 1 \pmod{41}$. Hence we use (mod 40) in reducing exponents and (mod 41) in reducing the bases in the equation $y^2 = 5^x + 31^x$. From equation (2.22) there are four possibilities modulo 40 : $x \equiv 9, 19, 29, 39 (\text{mod } 40)$. Let us use the fact that $5^3 \equiv 2 (\text{mod } 41)$, $31^3 \equiv 25 \pmod{41}$ and $5^{40} \equiv 31^{40} \equiv 1 (\text{mod } 41)$.

1. If $x \equiv 9 (\text{mod } 40)$, then, $y^2 = 5^x + 31^x \equiv 5^9 + 31^9 \equiv 8 + 4 \equiv 12 \pmod{41}$.
   But $\left(\frac{12}{41}\right) = \left(\frac{3}{41}\right).\left(\frac{4}{41}\right) = \left(\frac{3}{41}\right)$. Since $\left(\frac{4}{41}\right) = 1$ and $\left(\frac{3}{41}\right) = -1$, then $\left(\frac{12}{41}\right) = -1$.
2. If $x \equiv 19 \pmod{40}$, then, $y^2 = 5^x + 31^x \equiv 5^{19} + 31^{19} \equiv 33 + 4 \equiv 37 \pmod{41}$.
   Since $41 \equiv 37 \equiv 1 (\text{mod } 4)$, then $\left(\frac{37}{41}\right) = \left(\frac{41}{37}\right) = \left(\frac{4}{37}\right) = 1$.
3. If $x \equiv 29 (\text{mod } 40)$, then $y^2 = 5^x + 31^x \equiv 5^{29} + 31^{29} \equiv 8 + 4 \equiv 12 (\text{mod } 41)$ and hence $\left(\frac{12}{41}\right) = -1$ (see 1. above).
4. If $x \equiv 39 \bmod 40$, then $y^2 = 5^x + 31^x \equiv 5^{39} + 31^{39} \equiv 33 + 4 \equiv 37 \pmod{41}$ and hence $\left(\frac{37}{41}\right) = 1$ (see 2. above).

CONCLUSION:

The method used in proving Theorem 2.6 in analysing the Diophantine equation $y^2 = 5^x + 31^x$ in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ was working well from STEP 1 - 10 and it broke down in STEP11, where 2. and 4. in this step indicate that the equation $y^2 = 5^x + 31^x$ has two solutions modulo 41 in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ for $k \geq 1$, i.e $x \geq 3$, whilst for the equation $y^2 = 5^x + 11^x$ we found that it has no solution modulo 31 in the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ for $k \geq 1$. But that does not necessarily mean that those two modulo 41 solutions are integer solutions. The easiest two integer solutions to find are $(1, \pm 6)$. A further research may be pursued in finding whether there are other integer solutions for this exponential

Diophantine equation. ■

Chapter 3

p-adic Numbers

The aim of this chapter is to explain some concepts used in the estimates, lemmas and propositions on linear forms in two logarithms in archimedean and non archimedean metrics which are used in proving Theorem 4.1. As we will be dealing with the p-adic numbers, we have to define them. Our main focus will be on the theory of extension of a p-adic absolute values from $\mathbb{Q}$ to $\mathbb{Q}_p$. Finally we will be looking at finite field extensions of $\mathbb{Q}_p$ and this will lead us to residue fields. The references for this chapter are [8], [11] and [17].

3.1 Absolute Values

Our main focus in this section is non archimedean absolute values. We will look at the definition of an absolute value including the p-adic absolute value and what is meant when two absolute values are said to be equivalent. The theory in this section serves as a foundation for section 3.2 and 3.3. The references for this section are [8], [11] and [17].

Definition 3.1 *An absolute value on a field K is a function*

$$|\,.\,| : K \longrightarrow \mathbb{R}_+$$

that satisfies the following conditions:

(i) $|x| = 0$ *if and only if* $x = 0$,
(ii) $|xy| = |x|\,|y|$ *for all* $x, y \in K$ *and*
(iii) $|x + y| \leq |x| + |y|$ *for all* $x, y \in K$.
We say an absolute value on K *is non archimedean if it satisfies the additional condition*
(iv) $|x + y| \leq \max\{|x|, |y|\}$ *for all* $x, y \in K$.

Definition 3.2 *The absolute value* $|x| = 1$ *if* $x \neq 0$ *and* $|0| = 0$ *is called the trivial absolute value.*

Definition 3.3 *Fix a prime* p. *The* p*-adic valuation on* $\mathbb{Z}$ *is a function*

$$v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$$

defined as follows: for each integer $n \in \mathbb{Z}$, $n \neq 0$, *let* $v_p(n)$ *be a unique non negative integer satisfying* $n = p^{v_p(n)} \cdot u$ *where* $p \not| u$.
We extend v_p *to the field of rational numbers as follows: if* $x = \dfrac{a}{b} \in \mathbb{Q}^{\times}$ *then* $v_p(x) = v_p(a) - v_p(b)$. *We set* $v_p(0) = +\infty$.

Lemma 3.4 *The* p*-adic valuation satisfies the following properties: For all* $x, y \in \mathbb{Q}$ *we have*

1. $v_p(xy) = v_p(x) + \nu_p(y)$.
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ *with the equality occurring when* $v_p(x) \neq v_p(y)$.

Proof

1. Let $x = p^n \cdot u$ and $y = p^m \cdot u'$, where x and y are non zero elements in $\mathbb{Q}$ such that u and u' are not divisible by p. Then $xy = p^{m+n}(uu')$ and this implies that $v_p(xy) = m + n$, hence the assertion follows.

2. Using the same notation as before, suppose that $n < m$. Then $x+y = p^n(u + p^{m-n} \cdot u')$.

If $n < m$, then $u + p^{m-n} \cdot u'$ is not divisible by p, hence $v_p(x + y) = n$. If $n = m$, then it is possible that $u + p^{m-n} \cdot u' = u + u'$ is divisible by p, so the valuation of $(x + y)$ can be greater than n. This proves that $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$. ■

Definition 3.5 *For any $x \in \mathbb{Q}$ we define the p-adic absolute value of x by*

$$|x|_p = p^{-v_p(x)}$$

if $x \neq 0$ and $|0|_p = 0$.

Proposition 3.6 *The function $|\,.\,|_p$ is a non archimedean absolute value on $\mathbb{Q}$.*

Proof

From (2) in Lemma 3.4 we have

$$\begin{aligned} |x+y|_p &= p^{-v_p(x+y)} \\ &= p^{-\min\{v_p(x)\,,\,v_p(y)\}} \\ &\leq \max\left\{p^{-v_p(x)}\,,\,p^{-v_p(y)}\right\} \\ &\leq \max\left\{|x|_p\,,\,|y|_p\right\}. \end{aligned}$$

■

Proposition 3.7 *Let K be a field and let $|\,.\,|$ be a non archimedean absolute value on K. If $x, y \in K$ and $|x| \neq |y|$, then $|x+y| = \max\{|x|, |y|\}$.*

Proof

Suppose $|x| > |y|$. Since we have a non archimedean absolute value on K, then

$$|x+y| \leq \max\{|x|, |y|\} \leq |x|.$$

On the other hand we have

$$|x| = |(x+y)-y| \leq \max\{|x+y|, |y|\} \leq |x+y|$$

since $|x| \geq |y|$. This proves the theorem. ■

Proposition 3.8 *Let K be a field, $x \in K$ and $|\,.\,|$ the p-adic absolute value on K. If $|x| < 1$, then $\lim\limits_{n\to\infty} x^n = 0$ for $n \in \mathbb{N}$.*

Proof

Since $|x| < 1 \Rightarrow |x| \leq \dfrac{1}{p}$ and $|x^n| = |x|^n \leq \left(\dfrac{1}{p}\right)^n$. Then $\lim\limits_{n\to\infty} |x^n| = 0$ and hence $\lim\limits_{n\to\infty} x^n = 0$. ■

Definition 3.9 *An absolute value* $|\,.\,|$ *defines the metric* $d(x,y) = |x-y|$. *We say that the topology defined by this metric is the topology defined by* $|\,.\,|$.

Definition 3.10 *Two absolute values* $|\,.\,|_1$ *and* $|\,.\,|_2$ *on a field* K *are equivalent if they define the same topology on* K, *i.e if every set that is open with respect to one is also open with respect to the other.*

Lemma 3.11 *Let* $|\,.\,|_1$ *and* $|\,.\,|_2$ *be absolute values on a field* K. *Then the following conditions are equivalent:*
(i) There is an $\alpha > 0$ *such that for every* $x \in K$ *we have* $|x|_1 = |x|_2^{\alpha}$.
(ii) $|\,.\,|_1$ *and* $|\,.\,|_2$ *are equivalent absolute values.*
(iii) For any $x \in K$ *we have* $|x|_1 < 1 \iff |x|_2 < 1$.

Proof
(i)⇒(ii) Since $|x-a|_1 < r \Leftrightarrow |x-a|_2 < r^{1/\alpha}$. Hence topologies defined by $|\,.\,|_1$ and $|\,.\,|_2$ are the same.
(ii)⇒(iii) Since $|x|_1$ and $|x|_2$ define the same topology, $x^n \to 0$ in the $|\,.\,|_1$ topology ⇔ $x^n \to 0$ in the $|\,.\,|_2$ topology. Now $|x|_1 < 1 \Leftrightarrow x^n \to 0$ in the $|\,.\,|_1$ topology and similarly for $|\,.\,|_2$.
(iii)⇒(i). Let us assume $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$. Since $\left|\frac{1}{x}\right|_1 = \frac{1}{|x|_1}$, then if $\left|\frac{1}{x}\right|_1 < 1$ then $|x|_1 > 1$ and similarly for $|\,.\,|_2$. Hence $|x|_1 > 1 \Leftrightarrow |x|_2 > 1$ and consequently $|x|_1 = 1 \Leftrightarrow |x|_2 = 1$.
If $|\,.\,|_1$ is trivial, then $|x|_1 = 1$ for all $x \in K^{\times}$ and the same for $|\,.\,|_2$. Otherwise we can find $x_0 \in K^{\times}$ such that $|x_0|_1 \neq 1$ and we can replace x_0 by $\frac{1}{x_0}$ if necessary, such that if $|x_0|_1 < 1$ also $|x_0|_2 < 1$, so that there exist a positive real number α such that $|x_0|_1 = |x_0|_2^{\alpha}$.
Let us now choose any $x \in K^{\times}$. If $|x|_1 = |x_0|_1$ we must have also $|x|_2 = |x_0|_2$. So in this case the equation $|x|_1 = |x|_2^{\alpha}$ holds.
Suppose now $|x|_1 \neq 1$ and $|x|_i \neq |x_0|_i$ for $i = 1, 2$. As before choose β such that $|x|_1 = |x|_2^{\beta}$ and assume $|x|_1 < 1$ and hence by (iii) $|x|_2 < 1$. What we want to show is $\alpha = \beta$.
Let n and m be positive integers such that $|x^n|_1 < |x_0^m|_1$. Then

$$|x|_1^n < |x_0|_1^m \Leftrightarrow \frac{|x|_1^n}{|x_0|_1^m} < 1 \Leftrightarrow \left|\frac{x^n}{x_0^m}\right|_1 < 1 \Leftrightarrow \left|\frac{x^n}{x_0^m}\right|_2 < 1 \Leftrightarrow |x|_2^n < |x_0|_2^m .$$

Taking logs (logs are negative as $|\,.\,|_i < 1, i = 1, 2$) of the first and the last equations above, we have

$$n \log |x|_1 < m \log |x_0|_1 \iff n \log |x|_2 < m \log |x_0|_2$$

which can be written as

$$\frac{n}{m} > \frac{\log |x_0|_1}{\log |x|_1} \iff \frac{n}{m} > \frac{\log |x_0|_2}{\log |x|_2}.$$

Hence we get

$$\frac{\log |x_0|_1}{\log |x|_1} = \frac{\log |x_0|_2}{\log |x|_2}.$$

Thus

$$\alpha = \frac{\log |x_0|_1}{\log |x_0|_2} = \frac{\log |x|_1}{\log |x|_2} = \beta.$$

If we had $\frac{\log |x_0|_1}{\log |x|_1} < \frac{\log |x_0|_2}{\log |x|_2}$, then there is a rational $\frac{\log |x_0|_1}{\log |x|_1} < \frac{m}{n} < \frac{\log |x_0|_2}{\log |x|_2}$ which contradicts the above. ■

3.2 The field of p-adic numbers, $\mathbb{Q}_p$

In this section we look at the definition of the field of p-adic numbers ($\mathbb{Q}_p$) and properties of its elements. We also define a set of p-adic integers, $\mathbb{Z}_p$, which is a subset of $\mathbb{Q}_p$, and conclude by the definition of p-adic units in $\mathbb{Z}_p$. The main reference for this section is [8].

Different authors define $\mathbb{Q}_p$ in different ways. The approach that we will use to define $\mathbb{Q}_p$ will be in terms of Cauchy sequences. In this way it becomes clear that $\mathbb{Q}_p$ is a field. We first look at the following definitions of concepts from the basic topology.

Definition 3.12 *Let K be a field and let $|\,.\,|$ be an absolute value on K.*

1. *A sequence of elements $x_n \in K$ is called a Cauchy sequence if for every $\epsilon > 0$ we can find M such that we have $|x_n - x_m| < \epsilon$, whenever $m, n \geq M$.*

2. *A field K is called complete with respect to $|\,.\,|$ if every Cauchy sequence of elements of K has a limit in K.*

3. *A subset $S \subset K$ is called dense in K if every open ball around every element of K contains an element of S; in symbol, for every $x \in K$ and every $\epsilon > 0$ we have*

$$B(x, \epsilon) \cap S \neq \emptyset.$$

We now look on more theory on Cauchy sequences of rational numbers with respect to some absolute value and our objective is to find the completion of $\mathbb{Q}$ with respect to that absolute value.

Lemma 3.13 *A sequence of rational numbers (x_n) is a Cauchy sequence with respect to a non archimedean absolute value if and only if*

$$\lim_{n \to 0} |x_{n+1} - x_n| = 0.$$

Proof. See [[8], page 51]. ■

It is immediate from the above lemma we that a sequence of constants of rational numbers is a Cauchy sequence with respect to non archimedean absolute value.

Definition 3.14 *Two Cauchy sequences of rational numbers (a_i) and (b_i) are equivalent if $\lim_{i \to \infty} |a_i - b_i|_p = 0$.*

Lemma 3.15 *The field of rational numbers, $\mathbb{Q}$, is not complete with respect to any of its non trivial absolute values.*

Proof. See [[8], page 51 - 52]. ■

Since $\mathbb{Q}$ is not complete, our main aim is to extend $\mathbb{Q}$ to some field such that every Cauchy sequence in that field has a limit. Since different Cauchy sequences whose terms get close to each other are different objects as Cauchy sequences, this will require us to construct an equivalent class of Cauchy sequence on grounds that sequences in that class will have the same limit.

Before we define $\mathbb{Q}_p$, we first look at the following definitions and prove some lemmas and propositions on Cauchy sequences so as to make clear that $\mathbb{Q}_p$ is a field.

Definition 3.16 *Let $|\,.\,|_p$ be the non archimedean absolute value on $\mathbb{Q}$. We denote by $\mathcal{C}$ the set of all Cauchy sequences of elements of $\mathbb{Q}$ with respect to $|\,.\,|_p$.*

We will prove that $\mathcal{C}$ is a ring.

Proposition 3.17 *Defining*

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n) \cdot (y_n) = (x_n \cdot y_n)$$

make $\mathcal{C}$ a ring.

Proof
We prove by showing that the sequences $(x_n + y_n)$ and $(x_n \cdot y_n)$ are Cauchy with respect to non archimedean absolute value $|\,.\,|_p$.

Let (x_n) and (y_n) be Cauchy sequences in $\mathcal{C}$ with respect non archimedean absolute value $|\,.\,|_p$. Then for every $\epsilon, \epsilon' > 0$ there exists a positive integer N such that for $m, n > N$ $|x_n - x_m|_p < \epsilon$ and $|y_n - y_m|_p < \epsilon'$, hence

$$\begin{aligned} |(x_n + y_n) - (x_m + y_m)|_p &= |(x_n - x_m) + (y_n - y_m)|_p \\ &\leq \max\left\{|x_n - x_m|_p\,; |y_n - y_m|_p\right\} \\ &\leq |x_n - x_m|_p = |y_n - y_m|_p \text{ (by Proposition 3.7)} \\ &< \epsilon \end{aligned}$$

and

$$\begin{aligned} |x_n \cdot y_n - x_m \cdot y_m|_p &= |x_n\,(y_n - y_m) + y_m\,(x_n - x_m)|_p \\ &\leq \max\left\{|x_n\,(y_n - y_m)|_p\,; |y_m\,(x_n - x_m)|_p\right\} \\ &\leq \max\left\{|x_n|_p\,|(y_n - y_m)|_p\,; |y_m|_p\,|(x_n - x_m)|_p\right\} \\ &\leq |x_n|_p\,|y_n - y_m|_p = |y_m|_p\,|x_n - x_m|_p \text{ (by Proposition 3.7)} \\ &< \epsilon\epsilon'. \end{aligned}$$

We then conclude that the sequences $(x_n + y_n)$ and $(x_n \cdot y_n)$ are Cauchy with respect to non archimedean absolute value $|\,.\,|_p$. The conditions that addition and multiplication are commutative, associative and distributive follow immediately from the fact that $\mathbb{Q}$ is a ring. This completes the proof. ■

We now look for set of Cauchy sequences in $\mathcal{C}$ whose term get close to zero with respect to an absolute value $|\,.\,|_p$ on grounds that a class of Cauchy sequences who differ by elements in this set have the same limit and this will help us in the construction of the completion of $\mathbb{Q}$.

Definition 3.18 *We define $\mathcal{N} \subset \mathcal{C}$ to be*

$$\mathcal{N} = \left\{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\right\},$$

the subcollection of sequences that tends to zero with respect to the absolute value $|\,.\,|_p$.

We claim that $\mathcal{N}$ is an ideal of $\mathcal{C}$.

Proof

Let (x_n) and (y_n) be Cauchy sequences in $\mathcal{N}$. Then $\lim_{n\to\infty} |y_n|_p = 0$ and $\lim_{n\to\infty} |x_n|_p = 0$. But $|x_n + y_n|_p \leq |x_n|_p + |y_n|_p$ and $\lim_{n\to\infty} (|x_n|_p + |y_n|_p) = \lim_{n\to\infty} |x_n|_p + \lim_{n\to\infty} |y_n|_p = 0$. Hence $\lim_{n\to\infty} (|x_n + y_n|_p) = 0$. This implies that $(x_n + y_n) \in \mathcal{N}$ and hence $\mathcal{N}$ is closed under addition. The additive identity is (0) since $(x_n + 0) = (x_n)$ and the multiplicative identity is (1) since $(x_n \cdot 1)$. Let (z_n) be Cauchy sequence in $\mathcal{C}$. Then

$$\begin{aligned} \lim_{n\to\infty} |z_n x_n|_p &= \lim_{n\to\infty} |z_n x_n|_p \\ &\leq \lim_{n\to\infty} |z_n|_p \cdot \lim_{n\to\infty} |x_n|_p \\ &= 0, \end{aligned}$$

since $\lim_{n\to\infty} |x_n|_p = 0$, hence $(z_n x_n) \in \mathcal{N}$. This proves that $\mathcal{N}$ is an ideal of $\mathcal{C}$. ■

Lemma 3.19 *$\mathcal{N}$ is a maximal ideal of $\mathcal{C}$.*

Proof

Let $(x_n) \in \mathcal{C}$ be a Cauchy sequence that does not tends to zero with respect to the absolute value $|\,.\,|_p$ and let I be the ideal generated by (x_n) and $\mathcal{N}$. We want to show that I

must be all of $\mathcal{C}$.

Since (x_n) does not tends to zero with respect to the absolute value $|\,.\,|_p$ and is a Cauchy sequence, there exist a real number $c > 0$ and positive integer N such that $|x_n| \geq c > 0$ for $n \geq N$. This means that $x_n \neq 0$ for $n \geq N$. Let us define a new sequence (y_n) by setting $y_n = 0$ if $n < N$ and $y_n = \dfrac{1}{x_n}$ if $n \geq N$. Let us now check that (y_n) is a Cauchy sequence. But for $n \geq N$ we have

$$|y_{n+1} - y_n|_p = \left|\frac{1}{x_{n+1}} - \frac{1}{x_n}\right|_p \leq \left|\frac{x_{n+1} - x_n}{c^2}\right|_p \to 0.$$

From Lemma 3.13, this shows that (y_n) is a Cauchy sequence with respect to absolute value $|\,.\,|_p$. We notice that

$$x_n y_n = \begin{cases} 0 \text{ if } n < N \\ 1 \text{ if } n \geq N. \end{cases} \tag{3.1}$$

From the equation (3.1) we have $(1) - (x_n)(y_n) \in \mathcal{N}$, hence $(1) \in (x_n)(y_n) + \mathcal{N}$. This shows that (1) can be written as product of (x_n) plus an element of $\mathcal{N}$ and hence belongs to I. ■

We now define the field of p-adic numbers, $\mathbb{Q}_p$.

Definition 3.20 *We define the field of p-adic numbers to be the quotient of the ring $\mathcal{C}$ by its maximal ideal $\mathcal{N}$ i.e $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$.*

Since we have defined $\mathbb{Q}_p$ as a quotient ring, then we regard the elements of $\mathbb{Q}_p$ as equivalent class of Cauchy sequences. We have also proved in Lemma 3.19 that $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$, then $\mathbb{Q}_p$ is a field. We note that two different constant Cauchy sequences in $\mathbb{Q}$ never differ by an element in $\mathcal{N}$, but by another constant sequence. Two constant Cauchy sequences (x) and (x') in $\mathbb{Q}$ are equivalent if and only if $x = x'$ and this clear from Definition 3.14, hence we must have an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ by sending $x \in \mathbb{Q}$ to the equivalent class of the constant sequence (x) as our main objective is to extend $\mathbb{Q}$, this ensures that $\mathbb{Q}$ is a subset of $\mathbb{Q}_p$.

Definition 3.21 *If $\alpha \in \mathbb{Q}_p$ and (x_n) is any sequence representing α, we define $|\alpha|_p = \lim_{n\to\infty} |x_n|_p$.*

Lemma 3.22 *The set of value of $|\,.\,|_p$ on $\mathbb{Q}_p$ is $\{p^m : m \in \mathbb{Z}\} \cup \{0\}$.*

Proof

Let $x \in \mathbb{Q}_p$, $x \neq 0$ and (x_n) be a non zero Cauchy sequence in $\mathbb{Q}$ converging to x. Then $|x_n|_p = p^{m_n}$ for some $m_n \in \mathbb{Z}$. It immediate from Definition 3.21 that $|x|_p = \lim_{n\to\infty} p^{m_n} = p^m$ for some $m \in \mathbb{Z}$. ■

We have constructed $\mathbb{Q}_p$ and now we want to show elements of $\mathbb{Q}_p$. We use the following theorem which is stated without proof.

Theorem 3.23 *Every equivalent class of x in $\mathbb{Q}_p$ for which $|x|_p \leq 1$ has exactly one representative Cauchy sequence of the form (x_n) for which*

1. $x_n \in \mathbb{Z}$, $0 \leq x_n \leq p^n - 1$ for $n = 1, 2, 3 \cdots$.
2. $x_n \equiv x_{n-1}(\mod p^n)$ for $n = 1, 2, 3 \cdots$.

Proof. See [[11], page 11]. ■

Let us consider a case where x in $\mathbb{Q}_p$ but does not satisfy the condition $|x|_p \leq 1$. In this case we can multiply x by suitable power of p, say p^m, and we have $x' = p^m x$ which satisfies the condition $|x'|_p \leq 1$ and then $x = p^{-m}x'$. Then we have x' in $\mathbb{Q}_p$ and is represented by the sequence (x'_n) as in Theorem 3.23 and $x = p^{-m}x'$ is represented by the sequence (x_n). By Theorem 3.23 we can have $x'_n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1}p^{n-1}$ and $x'_{n+1} = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1}p^{n-1} + a_n p^n$, where $0 \leq a_n \leq p^n - 1$ for $n = 1, 2, 3 \cdots$. since $x_n \equiv x_{n-1}(\mod p^n)$. Then now we write x as powers of p as $x = a_0 p^{-m} + a_1 p^{1-m} + \cdots + a_{m-1}p^{-1} + a_m + a_{m+1}p + \cdots$ and we have both positive and negative powers of p. This equality is called the p-adic expansion of x.

Definition 3.24 *The ring of p-adic integers is the valuation ring*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

From the Definition 3.24 it is clear that $\mathbb{Z}_p$ is a set of elements of $\mathbb{Q}_p$ whose p-adic expansion involves non negative powers of p.

Definition 3.25 *The p-adic units are the invertible elements in* $\mathbb{Z}_p$.

We denote the set of p-adic units by $\mathbb{Z}_p^\times$. Let $x \in \mathbb{Z}_p$ be a unit. Since $x \in \mathbb{Z}_p$ means $|x|_p \leq 1$ and $|x^{-1}|_p = |x|_p^{-1} \leq 1 \Rightarrow |x|_p \geq 1$, hence $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p| : |x|_p = 1\}$. This shows that the p-adic units in $\mathbb{Z}_p^\times$ are elements in $\mathbb{Z}_p$ whose p-adic valuation is zero.

We have seen the construction of $\mathbb{Q}_p$, we now want to prove theoretically that $\mathbb{Q}_p$ is complete with respect to $|\,.\,|_p$. Before we prove that, we will state the following lemmas without proof and use them in our proof.

Lemma 3.26 *A sequence* (x_n) *in* $\mathbb{Q}_p$ *is a Cauchy sequence if and only if it satisfies*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0.$$

Proof. See [[8], page 88]. ■

Proposition 3.27 *The images of* $\mathbb{Q}$ *under the inclusion* $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ *is a dense subset of* $\mathbb{Q}_p$.

Proof. See [[8], page 57 - 58]. ■

Corollary 3.28 $\mathbb{Q}_p$ *is complete with respect to* $|\,.\,|_p$.

Proof

Let (λ_n) be a Cauchy sequence in $\mathbb{Q}_p$ representing λ. Then it is immediate from Lemma 3.27 that $\lim_{n\to\infty} |\lambda_{n+1} - \lambda_n|_p = 0$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we can find a sequence $(y_n) \in \mathbb{Q}$ such that $\lim_{n\to\infty} |\lambda_n - y_n|_p = 0$ and hence $|\lambda_n - y_n|_p \leq p^{-n}$.

We now prove that $(y_n) \in \mathbb{Q}$ is a Cauchy sequence with respect to $|\,.\,|_p$. We have

$$\begin{aligned} |y_{n+1} - y_n|_p &= |(y_{n+1} - \lambda_{n+1}) + (\lambda_{n+1} - \lambda_n) + (\lambda_n - y_n)|_p \\ &\leq \max\left\{|y_{n+1} - \lambda_{n+1}|_p\,; |\lambda_{n+1} - \lambda_n|_p\,; |\lambda_n - y_n|_p\right\} \\ &\leq \max\left\{p^{-(n+1)}; p^{-n}; p^{-n}\right\} \\ &= p^{-n}. \end{aligned}$$

Then $\lim_{n\to\infty} |y_{n+1} - y_n|_p = 0$ and hence (y_n) is a Cauchy sequence with respect to $|\,.\,|_p$.

We recall that we have (λ_n) as a Cauchy sequence in $\mathbb{Q}$, (hence in $\mathbb{Q}_p$, since $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$), representing $\lambda \in \mathbb{Q}_p$. Then by Definition 3.21 we have $\lim_{n\to\infty} |\lambda_n|_p = |\lambda|_p$ and hence $\lim_{n\to\infty} |\lambda_n - \lambda|_p = 0$. This implies that $\lim_{n\to\infty} \lambda_n = \lambda$. This proves that $\mathbb{Q}_p$ is complete with respect to $|\,.\,|_p$. ■

Finally we have a completion from $\mathbb{Q}$ to $\mathbb{Q}_p$ with respect to $|\,.\,|_p$ which have been constructed is such a way that it is a field. We recall from real analysis that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value, $|\,.\,|_\infty$.

We conclude this chapter by looking at the residue fields.

3.3 Finite Field Extensions of $\mathbb{Q}_p$ and Residue Fields

In this section we look at an absolute value on a finite field extension of $\mathbb{Q}_p$ that extends the p-adic absolute value on $\mathbb{Q}_p$ and the norm function from the finite field extension to its subfield. This leads us to derive formulae for calculating the absolute value and the valuation of an element of a finite field extension of $\mathbb{Q}_p$. We also prove the existence of an absolute value on the finite field extension of $\mathbb{Q}_p$. We will conclude this section by looking at the residue field. Once we have concluded this section, we will have covered most the terminology used in proving Theorem 4.1. The references for this chapter are [8], [11] and [17].

Before we prove Corollary 3.32, we look at the following definitions of terms which we will use in its proof.

Definition 3.29 *Let K be a complete valued field of characteristic zero with an absolute value $|\,.\,|$. A norm on a K vector space V is a function*

$$\|\,.\,\| : V \longrightarrow \mathbb{R}_+$$

that satisfies the following conditions:
(i) $||v|| = 0$ *if and only if* $v = 0$,
(ii) $||v + w|| \leq ||v|| + ||w||$ *for all* $v, w \in V$ *and*
(iii) $||\lambda v|| = |\lambda|\,||v||$ *for all for any* $v \in V$ *and* $\lambda \in K$.

Definition 3.30 *Two norms $||\,.\,||_1$ and $||\,.\,||_2$ are equivalent if there exist positive real numbers C and D such that for every $v \in V$, we have*

$$||v||_1 \leq C\,||v||_2 \text{ and } D\,||v||_2 \leq ||v||_1\,.$$

We will state Theorem 3.31 without proof and apply it in the proof of Corollary 3.32 and this corollary will help us in deriving the formula for calculating the absolute value of the elements of the finite field extension of $\mathbb{Q}_p$.

Theorem 3.31 *Let V be a finite-dimensional vector space over a complete field K. Then any two norms on V are equivalent.*

Proof. See [[11], page 58 - 59] or [[8], page 139 - 140]. ■

Corollary 3.32 *Let K be a finite extension of $\mathbb{Q}_p$. There is at most one absolute value on K which extends the p-adic absolute value on $\mathbb{Q}_p$.*

Proof
Suppose $|\,.\,|$ and $\|\,.\,\|$ are the two absolute values on K which extend the p-adic absolute value on $\mathbb{Q}_p$.
STEP 1

Let us prove that $|\,.\,|$and $\|\,.\,\|$ are equivalent.

Proof

To show that they are equivalent we need to show that for any $x \in K$ we have $|x| < 1 \Leftrightarrow \|x\| < 1$. But $|x| < 1$ if and only if $x^n \to 0$ with respect to the topology defined by $|\,.\,|$, similarily $\|x\| < 1$ if and only if $x^n \to 0$ with respect to the topology defined by $\|\,.\,\|$. But from Theorem 3.31, the absolute values $|\,.\,|$ and $\|\,.\,\|$ are equivalent as norms on a vector space K, hence define the same topology. Hence the the convergence with respect to one absolute value is exactly when we have the convergence with respect to the other. Hence $|\,.\,|$ and $\|\,.\,\|$ are equivalent.

STEP 2

Let us now prove that $|\,.\,| = \|\,.\,\|$.

Proof

Since $|\,.\,|$ and $\|\,.\,\|$ are equivalent, by Lemma 3.11 there exist a positive real number α such that for $x \in K$, we have $|x| = \|x\|^{\alpha}$. But $|x| = \|x\|$ whenever $x \in \mathbb{Q}_p$, since both absolute values extend the p-adic absolute value. Computing at $x = p$ shows that $\alpha = 1$ i.e the two absolute values are the same. Hence $|\,.\,| = \|\,.\,\|$. ■

Let K and F be fields such that $F \subset K$ and $[K : F]$ is finite. We now look at a function

$$N_{K/F} : K \longrightarrow F,$$

which is called a norm function from K to F. The norm function can be defined in several equivalent ways, each useful in certain contexts. Let us look the following three equivalent ways:

(i) Let $\alpha \in K$ and K/F a finite field extension and consider the F-linear map from K to K given by multiplication by α. Since this is linear, it corresponds to a matrix. Then we define $N_{K/F}(\alpha)$ to be the determinant of this matrix.

(ii) Let $\alpha \in K$ and consider the sub extension $F(\alpha)$. Set $r = [K : F(\alpha)]$ to be the degree of K as an extension of $F(\alpha)$. Let

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in F[X]$$

be the minimal polynomial of α over F . Then we define $N_{K/F}(\alpha) = (-1)^{nr} a_0^r$.
(iii) For K/F separable, $N_{K/F}(\alpha) = \prod \sigma(\alpha)$ where σ run through the finite set of all the isomorphisms of K/F.

Now let us compute the norm of an element of a field K using all the three definitions: Let $F = \mathbb{Q}_5$ and $K = \mathbb{Q}_5(\sqrt{7})$. Let us take a generic element $a + b\sqrt{7} \in K$. We first prove that $\sqrt{7} \notin \mathbb{Q}_5$. We prove by showing that 7 is not a square in $\mathbb{Q}_5$.
Proof
Contrary suppose 7 is a square in $\mathbb{Q}_5$. Then $7 = 2 + 1 \cdot 5 = (a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots)^2 \equiv a_0^2 \pmod 5$. This is impossible since $a_0^2 \equiv 0, 1, 4 \pmod 5$. Hence $\sqrt{7} \notin \mathbb{Q}_5$. ■

1. A basis of K over $\mathbb{Q}_5$ is $\{1, \sqrt{7}\}$. The linear map multiplication by $\alpha = a + b\sqrt{7}$ with respect to our basis yields the matrix:

$$A_\alpha = \begin{pmatrix} a & 7b \\ b & a \end{pmatrix}.$$

   Then $\det(A_\alpha) = a^2 - 7b^2$. Hence $N_{K/F}(\alpha) = a^2 - 7b^2$.

2. If $b = 0$ then $a + b\sqrt{7} \in \mathbb{Q}_5$ and $N_{K/F}(\alpha) = a^2$.
   If $b \neq 0$ we have $\left(a + b\sqrt{7}\right)^2 = a^2 + 7b^2 + 2ab\sqrt{7}$ and then $\left(a + b\sqrt{7}\right)^2 - 2a\left(a + b\sqrt{7}\right) + (a^2 - 7b^2) = 0$. Hence $X^2 - 2aX + (a^2 - 7b^2)$ is the minimal polynomial of $\alpha = a + b\sqrt{7}$. Hence $N_{K/F}(\alpha) = a^2 - 7b^2$.

3. We have two automorphisms i.e identity, i, and δ such that $i : a + b\sqrt{7} \mapsto a + b\sqrt{7}$ and $\delta : a + b\sqrt{7} \mapsto a - b\sqrt{7}$. Hence $N_{K/F}(\alpha) = \left(a + b\sqrt{7}\right)\left(a - b\sqrt{7}\right) = a^2 - 7b^2$.

In the following discourse we derive a formula for calculating the absolute value of an element of the finite extension field of $\mathbb{Q}_p$. We also show how this formula leads us to a formula for calculating the norm and valuation of an elements of the finite extension

fields of $\mathbb{Q}_p$.

Suppose $K/\mathbb{Q}_p$ is a normal extension and $[K:\mathbb{Q}_p]=n$. Let σ be an isomorphism of K, hence automorphism since $K/\mathbb{Q}_p$ is a normal extension and let $|\,.\,|$ be an absolute value on K extending the p-adic absolute value on $\mathbb{Q}_p$. Then the function $x \mapsto |\sigma(x)| = |x|$ for any $x \in K$, since by Theorem 3.32 there is at most one absolute value extension on $\mathbb{Q}_p$. Since $[K:\mathbb{Q}_p]=n$, multiplying over all σs, n of them, yields

$$\left|\prod_{\sigma}\sigma(x)\right| = |x|^n .$$

But

$$\left|\prod_{\sigma}\sigma(x)\right| = \left|N_{K/\mathbb{Q}_p}(x)\right|,$$

hence

$$|x| = \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x)\right|}.$$

If $x \in \mathbb{Q}_p$, we have $\sigma(x)=x$ and hence $N_{K/\mathbb{Q}_p}(x)=x^n$. Then $|x| = \sqrt[n]{|x^n|_p} = |x|_p$.

Since the absolute value of a norm is on $\mathbb{Q}_p$, then absolute value of a norm is p-adic and hence non archimedean by Proposition 3.6. From the above absolute value formulae we observe that $\nu_p(x) = \frac{1}{n}v_p\left(N_{K/\mathbb{Q}_p}(x)\right)$ and the absolute value of any non zero element $x \in K$ is of the form p^{ν} where $\nu \in \frac{1}{n}\mathbb{Z}$, since $v_p\left(N_{K/\mathbb{Q}_p}(x)\right) \in \mathbb{Z}$. This reduces the computing of ν_p to computing norms.

Example: Let K be a finite field extension of $\mathbb{Q}_2$. Suppose we want to compute $v_2(x)$ given $x = 1+\sqrt{5} \in K$. Then $N_{K/\mathbb{Q}_2}\left(1+\sqrt{5}\right) = -4$ and hence $v_2\left(N_{K/\mathbb{Q}_2}\left(1+\sqrt{5}\right)\right) = 2$. But $[K:\mathbb{Q}_2]=2$, hence $v_2(1+\sqrt{5}) = \frac{1}{2}(2) = 1$.

In Theorem 3.34 we prove the existence of an absolute value on a field K which extends the p-adic absolute value on $\mathbb{Q}_p$ and in our proof we will use Lemma 3.33 which is stated without proof.

Lemma 3.33 *If $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ is a monic irreducible polynomial with coefficients in $\mathbb{Q}_p$ and $a_0 \in \mathbb{Z}_p$, then all the coefficients $a_{n-1}, \ldots, a_1, a_0$ belong to $\mathbb{Z}_p$.*

Proof. See[[8], page 136 – 137]. ■

Theorem 3.34 *Let $K/\mathbb{Q}_p$ be a finite extension of degree n .*
The function $|\,.\,| : K \longrightarrow \mathbb{R}_+$ defined by

$$|x| = \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x)\right|_p},$$

is the unique non archimedean absolute value on K which extends the p-adic absolute value on $\mathbb{Q}_p$.

Proof
We have to check that all the conditions mentioned in Definition 3.1 are satisfied.
If $|x| = 0$, then $N_{K/\mathbb{Q}_p}(x) = 0$ and hence $x = 0$.
We have $N_{K/\mathbb{Q}_p}(xy) = N_{K/\mathbb{Q}_p}(x) \cdot N_{K/\mathbb{Q}_p}(y)$, as norms are multiplicative. Hence we have

$$\sqrt[n]{\left|N_{K/\mathbb{Q}_p}(xy)\right|_p} = \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x)\right|_p \cdot \left|N_{K/\mathbb{Q}_p}(y)\right|_p} = \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x)\right|_p} \cdot \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(y)\right|_p} = |x| \cdot |y|\,.$$

But if $x \in \mathbb{Q}_p$, then $N_{K/\mathbb{Q}_p}(x) = x^n$ so

$$|x| = \sqrt[n]{|x|_p^n} = |x|_p\,.$$

Now we have to prove the non archimedean inequality, i.e

$$|x + y| \leq \max\{|x|, |y|\}$$

for $x, y \in K$. Let $y \neq 0$ and $|x| \leq |y|$. Dividing through by y yields

$$\left|\frac{x}{y} + 1\right| \leq |x + 1| \leq \max\{|x|, 1\}\,.$$

This will be true if $|x| \leq 1 \Rightarrow |x - 1| \leq 1$. To see this we have to note that $x + 1 = -(-x - 1)$, hence if this implication is true, then we also have

$$|x| \leq 1 \Rightarrow |-x| \leq 1 \Rightarrow |-x - 1| = |x + 1| \leq 1.$$

Hence we need to prove that

$$N_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p \Rightarrow N_{K/\mathbb{Q}_p}(x-1) \in \mathbb{Z}_p.$$

We prove this using the definition of a norm in terms of the minimal polynomial.

Let $K = \mathbb{Q}_p(x)$ be the smallest field containing x. We use the fact that $\mathbb{Q}_p(x) = \mathbb{Q}_p(x-1)$, since any field containing x contains $(x-1)$ vice - versa. Let

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

be the minimal polynomial of x over $\mathbb{Q}_p$. Then the minimal polynomial of $x-1$ over $\mathbb{Q}_p$ is $f(X+1) = X^n + (a_{n-1}+n)X^{n-1} + \cdots + (1 + a_{n-1} + \cdots + a_1 + a_0)$. Using the definition (ii) of a norm, we have $N_{K/\mathbb{Q}_p}(x) = (-1)^n a_0$ and $N_{K/\mathbb{Q}_p}(x-1) = (-1)^n (1 + a_0 + \cdots + a_{n-1})$.

If $|x| \leq 1$, then $|a_0| = \sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x)\right|_p} \leq 1$ and $|a_0|_p \leq 1$, hence $\left|N_{K/\mathbb{Q}_p}(x)\right|_p \leq 1$. This implies that $a_0 \in \mathbb{Z}_p$ and hence $N_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p$. Since $f(X) \in \mathbb{Q}_p[X]$ and we have proved that $a_0 \in \mathbb{Z}_p$, it is immediate from Lemma 3.33 that $(1 + a_0 + \cdots + a_{n-1}) \in \mathbb{Z}_p$ and hence

$$\sqrt[n]{\left|N_{K/\mathbb{Q}_p}(x-1)\right|_p} = |1 + a_0 + \cdots + a_{n-1}|_p \leq 1.$$

This shows that $N_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p \Rightarrow N_{K/\mathbb{Q}_p}(x-1) \in \mathbb{Z}_p$. ■

Lastly we prove the following proposition which will lead us to the definition of a residue field of K.

Proposition 3.35 *Let K be a finite extension of $\mathbb{Q}_p$ and $[K : \mathbb{Q}_p] = n$. Let*
$A = \left\{x \in K : |x|_p \leq 1\right\}$
$M = \left\{x \in K : |x|_p < 1\right\}$

1. *Then A is a ring.*
2. *A is the integral closure of $\mathbb{Z}_p$ in K.*
3. *M is the unique maximal ideal of A.*

4. A/M is a finite extension of $\mathbb{F}_p$ of degree at most n.

Proof

1. Let $x, y \in A$. Then $|x|_p \leq 1$ and $|y|_p \leq 1$ and we have the following results: $|x-y|_p \leq \max\left\{|x|_p ; |y|_p\right\} \leq |x|_p = |y|_p \leq 1$, by Proposition 3.7. Then $x - y \in A$. But $|xy|_p = |x|_p \cdot |y|_p \leq 1 \Rightarrow xy \in A$ and $|-x|_p = |x|_p \leq 1 \Rightarrow -x \in A$. Then we can conclude that A is a ring.

2. In proving that A is integrally closed over $\mathbb{Z}_p$, let $\alpha \in K$ and $[K : \mathbb{Q}_p] = m$ and suppose α is integral over $\mathbb{Z}_p$. Then $\alpha^m + a_1\alpha^{m-1} + \cdots + a_n = 0$ for $a_i \in \mathbb{Z}_p$. Suppose $|\alpha|_p > 1$, then we have $|\alpha^m|_p = |a_1\alpha^{m-1} + \cdots + a_m|_p \leq \max\limits_{1\leq i\leq n} \left|a_i\alpha^{m-i}\right|_p \leq \max\limits_{1\leq i\leq n} \left|\alpha^{m-i}\right|_p = |\alpha|_p^{m-1}$. Hence $|\alpha|_p < 1$, a contradiction.
   Conversely, suppose $|\alpha|_p \leq 1$. Then all the conjugates of $\alpha = \alpha_1$ over $\mathbb{Q}_p$ also have $|\alpha_i|_p = \sqrt[m]{\left(\prod\limits_{j=1}^{m} |\alpha_j|_p\right)} = |\alpha|_p$, by Theorem 3.32. Since all coefficients in the monic irreducible polynomial are sums or differences of product α_i, it follows that these coefficients also have $|\,.\,|_p \leq 1$. Since they lie in $\mathbb{Q}_p$, hence they lie in $\mathbb{Z}_p$. Hence A is the integral closure of $\mathbb{Z}_p$ in K.

3. We now prove that M contains every proper ideal of A. Contrary suppose $\alpha \in A$ but $\notin M$. Then $|\alpha|_p = 1 \Rightarrow \left|\frac{1}{\alpha}\right|_p = 1 \Rightarrow \frac{1}{\alpha} \in A$. Hence any proper ideal containing α contains $\alpha.\frac{1}{\alpha} = 1$, which is impossible for a proper ideal. Hence M contains every proper ideal of A.

4. In proving that A/M is a finite extension of $\mathbb{F}_p$ of degree at most n, let us consider the following diagram:

$$\begin{array}{ccc} \mathbb{Q}_p & \subset & K \\ \bigcup & & \bigcup \\ \mathbb{Z}_p & \subset & A \\ \bigcup & & \bigcup \\ p\mathbb{Z}_p & \subset & M. \end{array}$$

Then we have the following: $\mathbb{Z}_p \cap M = p\mathbb{Z}_p$, $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow A/M \Rightarrow \mathbb{F}_p \subset A/M$ and $|\mathbb{F}_p| = p$. This means that A/M is an extension field over $\mathbb{F}_p$.

Now in proving that A/M has a finite degree over $\mathbb{F}_p$, let $[K : \mathbb{Q}_p] = n$. We show that any $n+1$ elements $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{n+1} \in A/M$ are linearly dependent over $\mathbb{F}_p$. Let a_i be any element in A which maps to $\overline{a}_i$ under the map $A \to A/M$. Since $[K : \mathbb{Q}_p] = n$ it follows that $a_1, a_2, \ldots, a_{n+1}$ are linearly dependent over $\mathbb{Q}_p$. Then if $a_1b_1 + a_2b_2 + \cdots + a_{n+1}b_{n+1} = 0$, $b_i \in \mathbb{Q}_p$, multiplying by a suitable power of p, we may assume that all $b_i \in \mathbb{Z}_p$, but at least one of the b_i is not in $p\mathbb{Z}_p$. The image of this expression in A/M is $\overline{a_1}\overline{b}_1 + \overline{a_2}\overline{b}_2 + \cdots + \overline{a_{n+1}}\overline{b}_{n+1} = 0$, where $\overline{b_i}$ is in $\mathbb{Z}_p/p\mathbb{Z}_p$. Since at least one of the b_i is not in $p\mathbb{Z}_p$, it follows that at least on of $\overline{b_i}$ is not zero. Hence $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_{n+1}$ are linearly dependent and $[A/M : \mathbb{F}_p] \leq n$. ■

Now from Proposition 3.35 we have the following:

Definition 3.36 *:*

1. *A/M is a field called the residue field of K.*

2. *The residue degree of the finite extension K of $\mathbb{Q}_p$ is the integer*

$$f = [A/M : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(A/M).$$

3. *The ramification index of K over $\mathbb{Q}_p$ is the integer*

$$e = \left[\left|K^\times\right| : \left|Q_p^\times\right|\right] = \left[\left|K^\times\right| : p^{\mathbb{Z}}\right] = \#\left(\left|K^\times\right|/p^{\mathbb{Z}}\right).$$

A finite extension K over $\mathbb{Q}_p$ is said to be:

1. *unramified when $e = 1$ i.e $[K : \mathbb{Q}_p] = f$ and*

2. *totally ramified when* $f = 1$ *i.e when* $[K : \mathbb{Q}_p] = n = e$.

We now want to prove that $ef = n$. Before we prove it, we have to look at the following definition and theorem which we will use in our proof. We also use the facts derived from Proposition 3.35 in our proof.

Definition 3.37 *Let* $K/\mathbb{Q}_p$ *be a finite extension and let* e *be the ramification index of* K *over* $\mathbb{Q}_p$. *We say an element* $\pi \in K$ *is a uniformizer if* $v_p(\pi) = \frac{1}{e}$.

Theorem 3.38 *Let* $K/\mathbb{Q}_p$ *be an algebraic extension of degree* n. *Let* O_K *be the ring of algebraic integers of* K. *Let* A *be a non zero integral ideal of* O_K. *Then*

$$N(A) = |(O_K/A)|.$$

Proof. See [[21], page $221 - 222$]. ■

Theorem 3.39 *Let* $K/\mathbb{Q}_p$ *be an algebraic extension of degree* n. *For each extension* K *over* $\mathbb{Q}_p$, *we have* $ef = [K : \mathbb{Q}_p] = n$.

Proof

From Definition 3.36, we have $[A/M : \mathbb{F}_p] = f$. We recall that $|\mathbb{F}_p| = p$ and hence $|(A/M)| = p^f$.

Now let π be a uniformizer of K, then from Definition 3.37 we have $v_p(\pi) = \frac{1}{e}$ and hence $ev_p(\pi) = v_p(\pi^e) = 1$. This implies that $v_p(\pi^e) = v_p(p) = 1$ for every prime number p. We recall that since p is a prime number, then $\langle p\rangle = \langle \pi^e\rangle$ is principal ideal of A. We have $\langle \pi^{i+1}\rangle \subset \langle \pi^i\rangle \subset A$, for $0 \leq i \leq e$. We infer that $\langle \pi^{i+1}\rangle \subset M$ and hence each quotient ring $\langle \pi^i\rangle / \langle \pi^{i+1}\rangle$ is isomorphic to A/M for each i. Taking $i = 0$, we have $\langle 1\rangle / \langle \pi\rangle$ and it is immediate from Theorem 3.38 that $|\langle 1\rangle / \langle \pi\rangle| = N(\pi) = p^f$. Since $\langle p\rangle = \langle \pi^e\rangle$, then $A/\langle p\rangle = A/\langle \pi^e\rangle$ and it is immediate from Theorem 3.38 that $|A/\langle p\rangle| = |A/\langle \pi^e\rangle| = N(\langle p\rangle) = N(\langle \pi^e\rangle)$. But $\langle 1\rangle / \langle \pi\rangle$ is isomorphic to A/M and $|A/M| = p^f$, hence $N(\langle \pi^e\rangle) = (N(\langle \pi\rangle))^e = \left(p^f\right)^e = p^{ef}$ and $N(\langle p\rangle) = p^n$, hence $n = ef$. ■

It is immediate from Theorem 3.39 that $f = \frac{n}{e}$.

We have covered in this chapter most of the theory on p-adic numbers which serves as a basic for the proof of Theorem 4.1 in the next chapter.

Chapter 4

The Diophantine Equation $x^2 - 2^m = y^n$

Introduction

The aim of this chapter is to analyse the proof by Y BUGEAUD in [1], where he corrects the results of Y.Guo and M.Le in [7] who unfortunately misused the results of Ping-Pong Dong by not considering the absolute value in $|\log \Lambda|$ in equation (14) of their proof as p-adic, hence that resulted in them claiming that the equation $x^2 - 2^m = y^n, \quad x, y, m, n \in \mathbb{N}, \gcd(x, y) = 1, \quad y > 1, \quad n > 2$ has only finitely many solutions, all satisfying $n < 2 \cdot 10^9$.

Before proving Theorem 4.1 we will prove Lemma 4.2 and 4.5 and Theorem 4.3 and apply Lemma 4.9, Propositions 4.11 and 4.12 without proof. Most of the theory on p-adic numbers which is used in this chapter is covered in more detail in chapter 3. The references for this chapter are [3], [7], [14], [15], [18], [19] and [21].

Theorem 4.1 *If (x, y, m, n) is a solution of the equation*

$$x^2 - 2^m = y^n \tag{4.1}$$

where $x, y, m, n \in \mathbb{N}$, $\gcd(x, y) = 1$, $y > 1$ and $n > 2$, then m and n are odd and the equation (4.1) has finitely many solutions satisfying $n \leq 5 \cdot 5 \times 10^5$.

4.1 Auxillary Results

Lemma 4.2 $\mathbb{Z}\left[\sqrt{2}\right]$ *has no units between*

$$1 \text{ and } 1+\sqrt{2}. \tag{4.2}$$

Proof

There are exactly two monomorphisms, say σ_1 and $\sigma_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$. These monomorphisms are given by $\sigma_1(x+y\sqrt{2}) = x+y\sqrt{2}$ and $\sigma_2(x+y\sqrt{2}) = x-y\sqrt{2}$ for all $x, y \in \mathbb{Q}$. Contrary let λ be a unit in $\mathbb{Z}\left[\sqrt{2}\right]$ such that

$$1 < \lambda < 1+\sqrt{2}. \tag{4.3}$$

Since λ is a unit, we have $\lambda|1$ such that

$$\lambda\mu = 1 \text{ for some } \mu \in \mathbb{Z}\left[\sqrt{2}\right]. \tag{4.4}$$

Let $\lambda' = \sigma_2(\lambda)$ and $\mu' = \sigma_2(\mu)$. Applying σ_2 to equation (4.4) we obtain

$$1 = \sigma_2(1) = \sigma_2(\lambda\mu) = \sigma_2(\lambda)\sigma_2(u) = \lambda'\mu'. \tag{4.5}$$

Hence

$$1 = (\lambda\lambda')(\mu\mu').$$

But $\lambda\lambda' \in \mathbb{Z}$ and $\mu\mu' \in \mathbb{Z}$ so that

$$\lambda\lambda' = \pm 1.$$

We consider two cases $\lambda\lambda' = 1$ and $\lambda\lambda' = -1$.

If $\lambda\lambda' = 1$. In this case by equation (4.3) we have

$$\sqrt{2}-1 = \frac{1}{1+\sqrt{2}} < \lambda' < 1. \tag{4.6}$$

Adding the inequalities in equation (4.3) and (4.6) yields

$$\sqrt{2} < \lambda + \lambda' < 2+\sqrt{2}$$

and thus

$$0.7 < \frac{1}{\sqrt{2}} < \frac{\lambda+\lambda'}{2} < 1 + \frac{1}{\sqrt{2}} < 1.8.$$

As $\frac{\lambda+\lambda'}{2} \in \mathbb{Z}$ we have $\frac{\lambda+\lambda'}{2} = 1$. From $\lambda\lambda' = 1$ and $\lambda + \lambda' = 2$. Hence $\lambda = \lambda' = 1$. This contradicts that $\lambda > 1$.

If $\lambda\lambda' = -1$ then by equation (4.3) we have

$$-1 < \lambda' < 1 - \sqrt{2}. \tag{4.7}$$

Adding the inequalities in equation (4.3) and (4.7) yields

$$0 < \lambda + \lambda' < 2,$$

hence

$$0 < \frac{\lambda+\lambda'}{2} < 1.$$

This is a contradiction as $\frac{\lambda+\lambda'}{2} \in \mathbb{Z}$. This completes the proof that there are no units of $\mathbb{Z}\left[\sqrt{2}\right]$ between 1 and $1+\sqrt{2}$. ■

Theorem 4.3 *All the units in* $\mathbb{Z}\left[\sqrt{2}\right]$ *are given by* $\pm\left(1+\sqrt{2}\right)^n$ *where* $n \in \mathbb{Z}$.

Proof

Let η be any unit in $\mathbb{Z}\left[\sqrt{2}\right]$ such that $\eta > 1$. Since there are no unit between 1 and $1+\sqrt{2}$ we must have $\eta \geq 1+\sqrt{2}$. Then there exist a unique positive integer n such that

$$(1+\sqrt{2})^n \leq \eta < (1+\sqrt{2})^{n+1}.$$

Thus

$$1 \leq \eta(1+\sqrt{2})^{-n} < (1+\sqrt{2}).$$

As $\eta(1+\sqrt{2})^{-n}$ is a unit in $\mathbb{Z}\left[\sqrt{2}\right]$, we have

$$\eta = (1+\sqrt{2})^n, n \in \mathbb{N}. \tag{4.8}$$

If η is a unit such that $0 < \eta < 1$, then $\frac{1}{\eta}$ is unit with $\frac{1}{\eta} > 1$. Hence, from equation (4.8) $\frac{1}{\eta} = (1+\sqrt{2})^n$ for some $n \in \mathbb{N}$, so that $\eta = (1+\sqrt{2})^{-n}, n \in \mathbb{N}$.

If η is a unit such that $-1 < \eta < 0$, then $\frac{-1}{\eta}$ is unit with $\frac{-1}{\eta} > 1$. Hence, from equation (4.8) $\frac{-1}{\eta} = (1+\sqrt{2})^n$ for some $n \in \mathbb{N}$, so that $\eta = -(1+\sqrt{2})^{-n}, n \in \mathbb{N}$.

If η is a unit such that $\eta < -1$, then $-\eta$ is unit with $-\eta > 1$. Hence, from equation (4.8) $-\eta = (1+\sqrt{2})^n$ for some $n \in \mathbb{N}$, so that $\eta = -(1+\sqrt{2})^n, n \in \mathbb{N}$.

Clearly

$$\pm 1 = \pm(1+\sqrt{2})^0.$$

Hence every unit in $\mathbb{Z}\left[\sqrt{2}\right]$ is given by $\eta = \pm\left(1+\sqrt{2}\right)^k, k \in \mathbb{Z}$. ■

The following definition was extracted from the explanation of a fundamental unit in [15].

Definition 4.4 *Let $K = \mathbb{Q}\left[\sqrt{2}\right]$ and ϵ be a unique unit in $\mathcal{O}_K$ such that $\epsilon > 1$ and every unit in $\mathcal{O}_K$ is of the form $\pm\epsilon^n$ where $n \in \mathbb{Z}$. Then ϵ is called a fundamental unit of $\mathcal{O}_K$.*

Lemma 4.5 *$\mathbb{Z}\left[\sqrt{2}\right]$ is a UFD.*

Proof

We will prove that $\mathbb{Z}\left[\sqrt{2}\right]$ is a UFD by showing that $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ is Euclidean.

Let $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$ and $y \neq 0$. Then$|N(xy)| = |N(x)| \cdot |N(y)|$ since the norm is multiplicative. Hence $|N(x)| \cdot |N(y)| > |N(y)|$.

Consider the number $\dfrac{x}{y} \in \mathbb{Q}\left[\sqrt{2}\right]$, so we may write $\dfrac{x}{y} = a' + b'\sqrt{2}$ with $a', b' \in \mathbb{Q}$. Let a and $b \in \mathbb{Z}$ be the best approximation to a' and b' i.e $|a'-a| \leq \frac{1}{2}, \quad |b'-b| \leq \frac{1}{2}$. Let $x = qy + r$, such that $q = a + b\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$. So

$r = \left[(a'-a) + (b'-b)\sqrt{2}\right](y) \in \mathbb{Q}\left[\sqrt{2}\right]$. Hence

$$\begin{aligned}
|N(r)| &= |N\left(\left[(a'-a)+(b'-b)\sqrt{2}\right]\right)N(y)| \\
&= |N\left[(a'-a)+(b'-b)\sqrt{2}\right]N(y)| \\
&\leq \left|(a'-a)^2 - 2(b'-b)^2\right| N(y) \\
&\leq \max\left|\left(\frac{1}{4}, \frac{1}{2}\right)\right| |N(y)| \\
&< \frac{1}{2}|N(y)| \\
&< |N(y)|.
\end{aligned}$$

Then $\mathbb{Z}\left[\sqrt{2}\right]$ is Euclidean and hence PID and UFD. ■

Definition 4.6 *For any integer x, we denote $P[x]$ its greatest prime factor.*

Lemma 4.7 *Let a, b, x and y be non zero integers with $(x, y) = 1$. Put $X = \max\{|x|, |y|\}$. For any integer $n \geq 3$, there exist computable constants c_1 and X_1, depending only on a, b and n, such that*

$$P\left[ax^2 + by^n\right] \geq c_1 \left((\log\log X \log\log\log X\right)^{\frac{1}{2}}$$

when $X \geq X_1$.

Proof. This is a particular case of a theorem due to Kotov [12]. ■

Lemma 4.8 *Let $k = k_1 k_2$ be a factorization of k such that the $\gcd(k_1, k_2) = 1$. Then the general integer solution of the equation*

$$XY = kZ^n, \text{ such that } \gcd(X, Y) = 1, \ Z \neq 0, \ n \in \mathbb{Z},$$

is given by

$$X = \pm k_1 P^n, \ Y = \pm k_2 Q^n,$$

where P and Q are arbitrary integers such that $Z = \pm PQ$ with $\gcd(k_1 P^n, k_2 Q^n) = 1$.

Proof. See [[15], page 16]. ■

Lemma 4.9 *The equation $2^m - y^n = 1$ has no solution with $y > 1$ and $n \geq 2$.*

Proof. This lemma immediately follows from Satz 3 of Hyyrö [9]. ■

Definition 4.10 *Two algebraic numbers k and l are said to be multiplicatively dependent if there exist two non zero integers m and n such that $k^m = l^n$, otherwise k and l are multiplicatively independent.*

The next two propositions deal with the lower bounds for the linear forms in two logarithms. Let $\alpha = \alpha_1$ be a non zero algebraic number with defining minimal polynomial $a_0 (X - \alpha_1) \cdots (X - \alpha_n)$ over $\mathbb{Z}$. The logarithm height of α, denoted by $h(\alpha)$ is defined by

$$h(\alpha) = \frac{1}{n} \log \left(a_0 \prod_{i=1}^{n} \max\{1, |\alpha_i|\} \right).$$

For any prime number p, let $\overline{\mathbb{Q}}_p$ be an algebraic closure of the field $\mathbb{Q}_p$ of p-adic numbers. We denote by ν_p the unique extension to $\overline{\mathbb{Q}}_p$ of the p-adic evaluation over $\mathbb{Q}_p$, normalized by $\nu_p(p) = 1$. For more details on p-adic numbers see chapter 3.

Proposition 4.11 *Let p be a prime number. Let α_1 and α_2 be two algebraic numbers which are p-adic units. Denote by f the residual degree of the extension $\mathbb{Q}_p \hookrightarrow \mathbb{Q}_p(\alpha_1, \alpha_2)$ and put $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/f$. Let b_1 and b_2 be two positive integers and put*

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2}.$$

Denote by $A_1 > 1$ and $A_2 > 1$ two real numbers such that

$$\log A_i \geq \max\{h(\alpha_i), \frac{\log p}{D}\}, \quad i = 1, 2,$$

and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the lower bound

$$v_p(\Lambda) \leq \frac{18p(p^f - 1)}{(p-1)(\log p)^4} \cdot D^4 \left(\max \left\{ \log b' + \log \log p + 0.4, \ \frac{15 \log p}{D}, 10 \right\} \right)^2 \log A_1 \log A_2.$$

Proof. This is Théorèm 4 of [2] with the choice $(\mu, \nu) = (10, 15)$. ∎

Proposition 4.12 *Let $\alpha_1 \geq 1$ and $\alpha_2 \geq 1$ be two real algebraic numbers. Let b_1 and b_2 be two positive integers and put*

$$\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2.$$

Set $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ and denote by $A_1 > 1$ and $A_2 > 1$ two real numbers satisfying

$$\log A_i \geq \max\{h(\alpha_i), \frac{1}{D}\}, \quad i = 1, 2.$$

Finally, put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the lower bound

$$\log |\Lambda| \geq -24.7 D^4 (\max\{\log b' + 0.18, 0.5, \frac{20}{D}\})^2 \log A_1 \log A_2.$$

Proof. This is a Corollaire 2 of [13]. ∎

4.2 Proof of Theorem 4.1

STEP 1: An elementary analysis of the equation $x^2 - 2^m = y^n$.

We claim that x and y are odd.

Proof

Let x be even say $x = 2p$ for some $p \in \mathbb{N}$. Then substituting in equation (4.1) yields $2\left(2p^2 - 2^{m-1}\right) = y^n$. This implies that y is even. We have a contradiction since the $\gcd(x, y) = 1$. Similarly if y is even, x is even and this leads to a contradiction. Then we can conclude that x and y are odd. ■

Let us show why the hypothesis $n > 2$ in the equation (4.1) is necessary.

Contrary suppose $n = 2$. Then we have $x^2 - y^2 = (x-y)(x+y) = 2^m$. Since x and y are odd $(x-y)$ and $(x+y)$ are even. From the equation $(x-y)(x+y) = 2^m$ we can have $\frac{(x-y)}{2} \cdot \frac{(x+y)}{2} = 2^{m-2}$.

We claim that $\frac{(x-y)}{2}$ and $\frac{(x+y)}{2}$ are co-prime.

Suppose the $\gcd\left(\frac{(x-y)}{2}, \frac{(x+y)}{2}\right) = d > 1$. This implies that $d|\frac{(x-y)}{2}$ and $d|\frac{(x+y)}{2}$ and hence $d|\left(\frac{(x-y)}{2} + \frac{(x+y)}{2}\right)$ and this implies that $d|x$ and hence d is odd since x is odd. Then from equation $\frac{(x-y)}{2} \cdot \frac{(x+y)}{2} = 2^{m-2}$ this implies that $d^2|2^{m-2}$ and $d|2^{m-2}$, hence d is even, a contradiction. This proves the claim that $\frac{(x-y)}{2}$ and $\frac{(x+y)}{2}$ are co-prime.

Since the $\gcd\left(\frac{(x-y)}{2}, \frac{(x+y)}{2}\right) = 1$, from equation $\frac{(x-y)}{2} \cdot \frac{(x+y)}{2} = 2^{m-2}$ we can have $\frac{(x-y)}{2} = 1$ and $\frac{(x+y)}{2} = 2^{m-2}$ or $\frac{(x-y)}{2} = 2^{m-2}$ and $\frac{(x+y)}{2} = 1$. If $\frac{(x-y)}{2} = 1$ and $\frac{(x+y)}{2} = 2^{m-2}$, we have the system of equations $x - y = 2$ and $x + y = 2^{m-1}$ and this yields the solution $(x, y) = (2^{m-2} + 1\,, 2^{m-2} - 1)$.

We now check whether $(x, y) = (2^{m-2} + 1\,, 2^{m-2} - 1)$ is a solution of the equation (4.1) for all $m > 2$. For $m \geq 3$ we have $y \geq 1$. We have a contradiction if $y = 1$ since from the hypothesis we have $y > 1$ and if $m > 3$, $(x, y) = (2^{m-2} + 1\,, 2^{m-2} - 1)$ has infinitely many solutions and hence the equation (4.1) has infinitely many solutions. However we will prove later in the conclusion that the equation (4.1) has finitely many solutions, hence we

have a contradiction.

For $\frac{(x-y)}{2} = 2^{m-2}$ and $\frac{(x+y)}{2} = 1$, we have the system of equations $x - y = 2^{m-1}$ and $x + y = 2$ and this yields the solution $(x, y) = (2^{m-2} + 1\,, 1 - 2^{m-2})$ and for $m > 2$ we have $y \leq -1$, a contradiction since we must have $y > 1$. ■

We claim that n and m are odd.

Proof

Suppose n is even, say $n = 2t$ for some $t \in \mathbb{N}$. Then from equation (4.1) we have $(x + y^t)\,(x - y^t) = 2^m$. Since x and y are odd, both $x + y^t$ and $x - y^t$ are even. We can write equation (4.1) as $\frac{(x+y^t)}{2} \cdot \frac{(x-y^t)}{2} = 2^{m-2}$. Using the same procedure as in the above proof, we can prove that the gcd $\left(\frac{(x-y^t)}{2}, \frac{(x+y^t)}{2}\right) = 1$. We can have $\frac{(x+y^t)}{2} = 2^{m-2}$ and $\frac{(x-y^t)}{2} = 1$ and this leads to the system of equations $x - y^t = 2$ and $x + y^t = 2^{m-1}$. Subtracting $x - y^t = 2$ from $x + y^t = 2^{m-1}$ yields $2^{m-2} - y^t = 1$. From Lemma 4.9, this equation has no solution. Hence n should be odd.

Suppose m is even, say $m = 2q$ for some $q \in \mathbb{N}$. Then from equation (4.1), we have $(x - 2^q)(x + 2^q) = y^n$ and $2 \not| xy$ as x and y are odd integers.

Let us first prove that $x - 2^q$ and $x + 2^q$ are co-prime. Suppose $\gcd(x - 2^q, x + 2^q) = d > 1$, where $d \in \mathbb{N}$. Then $d|(x - 2^q)$ and $d|(x + 2^q)$ and hence $d|[(x - 2^q) + (x + 2^q)]$ this implies that $d|2x$ and hence $d|2$ or $d|x$. From the equation $(x - 2^q)(x + 2^q) = y^n$ this also implies that $d^2|y^n$, hence $d|y^n$. If $d|2$ this implies that $d = 2$ and $2|y^n$, a contradiction since y^n is odd as y is odd. If $d|x$ and $d|y^n$ we have a contradiction since $\gcd(x, y) = 1$. Then we can conclude that the $\gcd(x - 2^q, x + 2^q) = 1$, hence $x - 2^q$ and $x + 2^q$ are co-prime. From the equation $(x - 2^q)(x + 2^q) = y^n$ and by Lemma 4.8 we can have $x + 2^q = y_1^n$ and $x - 2^q = y_2^n$ where $y_1 \cdot y_2 = y$ such that the $\gcd(y_1, y_2) = 1$. Since y is odd, then y_1 and y_2 are odd. Subtracting $x - 2^q = y_2^n$ from $x + 2^q = y_1^n$ yields

$$\begin{aligned} 2^{q+1} &= y_1^n - y_2^n \\ &= \frac{y_1^n - y_2^n}{y_1 - y_2} \cdot (y_1 - y_2). \end{aligned} \tag{4.9}$$

$y_1 - y_2$ is even as y_1 and y_2 are odd.

We claim that $\dfrac{y_1^n - y_2^n}{y_1 - y_2}$ is odd.

Proof

Since $y_1 - y_2$ is even, we have $y_1 \equiv y_2 \pmod 2$ and

$$\begin{aligned}\frac{y_1^n - y_2^n}{y_1 - y_2} &= y_1^{n-1} + y_1^{n-2} \cdot y_2 + \cdots + y_2^{n-1} \\ &\equiv y_1^{n-1} + y_1^{n-2} \cdot y_1 + \cdots + y_1^{n-1} \pmod 2 \\ &\equiv n y_1^{n-1} \pmod 2 \\ &\not\equiv 0 \pmod 2 \text{ since } n \text{ and } y_1 \text{ are odd.}\end{aligned}$$

This implies that $\dfrac{y_1^n - y_2^n}{y_1 - y_2}$ is odd. Then from equation (4.9) we can have $\dfrac{y_1^n - y_2^n}{y_1 - y_2} = 1$ and $y_1 - y_2 = 2^{q+1}$. But for $\dfrac{y_1^n - y_2^n}{y_1 - y_2} = 1$, this is impossible since $n \geq 3$. This proves that both m and n are odd integers. ■

Let $K = \mathbb{Q}[\sqrt{2}]$. Now let us factorize $x^2 - 2^m = y^n$ working in the ring $\mathbb{Z}\left[\sqrt{2}\right]$, the ring of algebraic integers in K. We have also proved in Lemma 4.5 that $\mathbb{Z}\left[\sqrt{2}\right]$ is PID, hence UFD.

Let $\langle\alpha\rangle$ be the principal ideal of $\mathbb{Z}\left[\sqrt{2}\right]$ generated by α. Then from the equation $x^2 - 2^m = y^n$ factorising the LHS in $\mathbb{Z}\left[\sqrt{2}\right]$ we have $\left(x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right)\left(x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right) = y^n$. Passing to ideals we get

$$\left\langle x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle \left\langle x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle = \langle y\rangle^n . \tag{4.10}$$

We claim that $\left\langle x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ and $\left\langle x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ are co-prime.

Proof

Contrary suppose $\left\langle x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ and $\left\langle x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ are not co-prime. Let P be a prime ideal of $\mathbb{Z}\left[\sqrt{2}\right]$ such that $P \mid \left\langle x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ and $P \mid \left\langle x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$. Then $P^2 \mid \langle y\rangle^n$ and hence $P \mid \langle y\rangle$. We then have $\left\langle x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle \in P$, $\left\langle x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle \in P$ and $\langle y\rangle \in P$. This implies that $\left(x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right) \in P$, $\left(x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right) \in P$ and $y \in P$. Hence $\left(x + 2^{\frac{(m-1)}{2}}\sqrt{2}\right) + \left(x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right) = 2x \in P$. Since $\gcd(x, y) = 1 \Rightarrow \gcd(2x, y) = 1$.

This implies that there exist non zero elements of $\mathbb{Z}$, say l and k such that $(2x)l+(y)k = 1 \in P$. This is impossible since $\mathbb{Z}\left[\sqrt{2}\right] \neq P$. This proves that $\left\langle x+2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ and $\left\langle x-2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle$ are co-prime and hence
$\gcd\left(\left\langle x+2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle, \left\langle x-2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle\right) = \langle 1\rangle$. ■

Then from the equation (4.10) we have

$$\left\langle x+2^{\frac{(m-1)}{2}}\sqrt{2}\right\rangle = \langle\beta\rangle^n \tag{4.11}$$

for $\beta \in \mathbb{Z}\left[\sqrt{2}\right]$. Let $\rho = 1+\sqrt{2}$ be the fundamental unit of $\mathbb{Z}\left[\sqrt{2}\right]$. We have proved in Theorem 4.3 that all the units in $\mathbb{Z}\left[\sqrt{2}\right]$ are in the form $\pm\rho^u$, where u is an integer. Using Theorem 2.5 and equation (4.11) we have

$$x+2^{\frac{(m-1)}{2}}\sqrt{2} = \pm\beta^n\rho^u. \tag{4.12}$$

Using Euclidean division we can write $u = qn-t$ where $q, u \in \mathbb{Z}$, $n \in \mathbb{N}$ and $0 < t \leq n$. Since n is odd, then $-1 = (-1)^n$ and hence we can write $\pm\beta^n\rho^u = \left(a+b\sqrt{2}\right)^n\rho^{-t}$, where $a, b \in \mathbb{Z}$. Then from the equation (4.12) the substitution of $\pm\beta^n\rho^u$ yields

$$x+2^{\frac{(m-1)}{2}}\sqrt{2} \;=\; \left(a+b\sqrt{2}\right)^n\rho^{-t}. \tag{4.13}$$

Finding conjugates in equation (4.13) yields

$$x-2^{\frac{(m-1)}{2}}\sqrt{2} = \left(a-b\sqrt{2}\right)^n\bar{\rho}^{-t}. \tag{4.14}$$

We claim that $y = (a^2-2b^2)(-1)^t$.

Proof

From equations (4.13) and (4.14) we have

$$y^n = \left(x+2^{\frac{(m-1)}{2}}\sqrt{2}\right)\left(x-2^{\frac{(m-1)}{2}}\sqrt{2}\right) = \left(a^2-2b^2\right)^n(\rho\bar{\rho})^{-t}.$$

But $\rho\cdot\bar{\rho} = (1+\sqrt{2})(1-\sqrt{2}) = -1$, then $y^n = (a^2-2b^2)^n(-1)^t$ since $(-1)^{-t} = (-1)^t$. If t is odd $(-1)^t = -1$ and hence $(-1)^{nt} = -1$ since n is odd and if t is even $(-1)^{nt} = 1$, so $y = (a^2-2b^2)(-1)^t$ depending on whether t is even or odd.

We define

$$\tau = \begin{cases} 1 & \text{if } t \text{ is even} \\ -1 & \text{if } t \text{ is odd,} \end{cases}$$

so we have $y = \tau\,(a^2 - 2b^2)$. ■

We claim that a is odd and a and b are co-prime.

Proof

We have $y = \tau(a - b\sqrt{2})(a + b\sqrt{2}) = \tau(a^2 - 2b^2)$. We have proved that y is odd, but $2b^2$ is always even for all values of b then a^2 is odd hence a.

We now prove that a and b are co-prime.

Contrary suppose a and b are not co-prime. Let $\gcd(a, b) = d > 1$ where $d \in \mathbb{N}$. Then we can have $a = dk$ and $b = dl$ such that $\gcd(k, l) = 1$ where $k, l \in \mathbb{N}$. Substitution in equation (4.13) yields

$$\begin{aligned} x + 2^{\frac{(m-1)}{2}}\sqrt{2} &= d^n\left(k + l\sqrt{2}\right)^n \rho^{-t} \\ \frac{x}{d^n} + \frac{2^{\frac{m-1}{2}}}{d^n}\sqrt{2} &= \left(k + l\sqrt{2}\right)^n \rho^{-t}. \end{aligned}$$

But $\left(k + l\sqrt{2}\right)^n \rho^{-t} \in \mathbb{Z}\left[\sqrt{2}\right]$ and $\frac{x}{d^n} + \frac{2^{\frac{m-1}{2}}}{d^n}\sqrt{2} \notin \mathbb{Z}\left[\sqrt{2}\right]$ since $\gcd\left(x, 2^{\frac{m-1}{2}}\right) = 1$ and d^n cannot divide both x and $2^{\frac{m-1}{2}}$. This proves that a and b are co-prime. ■

We claim that $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > \left|x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right|$ and hence $a + b\sqrt{2} > \left|a - b\sqrt{2}\right|$.

Proof

We have to first show that $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > x - 2^{\frac{(m-1)}{2}}\sqrt{2}$ and $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > -x + 2^{\frac{(m-1)}{2}}\sqrt{2}$. But $x > 0$ and $2^{\frac{(m-1)}{2}} > 0$ and $2^{\frac{(m-1)}{2}}\sqrt{2} > -2^{\frac{(m-1)}{2}}\sqrt{2}$. Hence $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > 0$ and $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > x - 2^{\frac{(m-1)}{2}}\sqrt{2}$.

Since $x > -x$, then $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > -x + 2^{\frac{(m-1)}{2}}\sqrt{2}$. Hence $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > \left|x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right|$ for all values of x and m.

Since $x + 2^{\frac{(m-1)}{2}}\sqrt{2} > \left|x - 2^{\frac{(m-1)}{2}}\sqrt{2}\right|$, then from RHS of equations (4.13) and (4.14)

$$\left(a + b\sqrt{2}\right)^n \rho^{-t} > \left|\left(a - b\sqrt{2}\right)^n \rho^{t}\right|. \tag{4.15}$$

This implies that

$$\left(a + b\sqrt{2}\right)^n > \left|a - b\sqrt{2}\right|^n \rho^{2t} > \left|a - b\sqrt{2}\right|^n \tag{4.16}$$

and hence $a+b\sqrt{2} > \left|a-b\sqrt{2}\right|$. ■

We claim that $a > 0$ and $b > 0$ and hence $a+b\sqrt{2} > 0$.

Proof

Since $a+b\sqrt{2} > \left|a-b\sqrt{2}\right|$, then by the definition of archimedean absolute value inequality we have $a+b\sqrt{2} > a-b\sqrt{2}$ and $a+b\sqrt{2} > -a+b\sqrt{2}$. Then $2b\sqrt{2} > 0$ and $2a > 0$ and hence $b > 0$ and $a > 0$. This implies that $a+b\sqrt{2} > 0$. ■

Since $y = \tau(a-b\sqrt{2})(a+b\sqrt{2})$ and we are given from the hypothesis that $y > 1$ and we have proved that $a+b\sqrt{2} > 0$, then we can also conclude that $\tau(a-b\sqrt{2}) > 0$.

Finally let $\epsilon = a+b\sqrt{2}$ such that ϵ is not a unit in $\mathbb{Z}\left[\sqrt{2}\right]$. Then from equation (4.13) and (4.14) we get

$$\begin{cases} x + 2^{\frac{(m-1)}{2}}\sqrt{2} = \epsilon^n \rho^{-t}, \\ x - 2^{\frac{(m-1)}{2}}\sqrt{2} = (\tau\overline{\epsilon})^n \rho^t. \end{cases} \tag{4.17}$$

From the system of equations in (4.17) subtracting the two the equations yields

$$2^{\frac{(m+1)}{2}}\sqrt{2} = \epsilon^n \rho^{-t} - (\tau\overline{\epsilon})^n \rho^t. \tag{4.18}$$

Dividing equation (4.18) by $(\tau\overline{\epsilon})^n \rho^{-t}$ yields

$$\left(\frac{\epsilon}{\tau\overline{\epsilon}}\right)^n - \rho^{2t} = \frac{2^{\frac{(m+1)}{2}}\sqrt{2}}{(\tau\overline{\epsilon})^n \rho^{-t}} = \frac{2^{\frac{m+2}{2}}}{(\tau\overline{\epsilon})^n \rho^{-t}}. \tag{4.19}$$

Let

$$A_u = \left(\frac{\epsilon}{\tau\overline{\epsilon}}\right)^n - \rho^{2t}. \tag{4.20}$$

Since we have proved that a is odd then $\nu_2(\tau\overline{\epsilon}) = 0$ and we have also $v_2\left(\rho^{-1}\right) = v_2(\sqrt{2}-1) = 0$, hence $\nu_2(A_u) = \dfrac{m+2}{2}$.

We now calculate the logarithmic heights of $\dfrac{\epsilon}{\tau\overline{\epsilon}}$ and $\rho^2 = 3+2\sqrt{2}$.

Let us find a polynomial of degree 2 such that $\dfrac{\epsilon}{\tau\overline{\epsilon}}$ is a root of that polynomial. We have

two automorphisms in $\mathbb{Z}\left[\sqrt{2}\right]$, the identity and $\delta : \frac{\epsilon}{\tau\bar{\epsilon}} \rightarrow \frac{\bar{\epsilon}}{\tau\epsilon}$. Then we have

$$\begin{aligned}\left(X - \frac{\epsilon}{\tau\bar{\epsilon}}\right)\left(X - \frac{\bar{\epsilon}}{\tau\epsilon}\right) &= 0 \\ \epsilon\bar{\epsilon}X^2 - \tau\left(\epsilon^2 + \bar{\epsilon}^2\right)X + \epsilon\bar{\epsilon} &= 0.\end{aligned}$$

Let $f(X) = \epsilon\bar{\epsilon}X^2 - \tau\left(\epsilon^2 + \bar{\epsilon}^2\right)X + \epsilon\bar{\epsilon}$. We claim that the coefficients of f are in $\mathbb{Z}$ and are co-prime.

Proof

Since $\epsilon = a + b\sqrt{2}$, we have $\bar{\epsilon}\epsilon = (a^2 - 2b^2)$ and $\tau(\epsilon^2 + \bar{\epsilon}^2) = \tau(2a^2 + 4b^2)$ where $a, b \in \mathbb{Z}$, hence $\bar{\epsilon}\epsilon$ and $\tau(\epsilon^2 + \bar{\epsilon}^2)$ are in $\mathbb{Z}$.

We have proved that a is odd and a and b are co-prime, hence $\bar{\epsilon}\epsilon = (a^2 - 2b^2)$ is odd, since a^2 is odd and $2b^2$ is even. But $\tau(\epsilon^2 + \bar{\epsilon}^2) = 2\tau(a^2 + 2b^2)$, which is even and we have proved that $\bar{\epsilon}\epsilon$ is odd, hence the $\gcd\left(\epsilon\bar{\epsilon}, \tau\left(\epsilon^2 + \bar{\epsilon}^2\right)\right) = 1$. ■

We have proved that coefficients of f are co-prime and hence we can calculate the logarithmic height of $\frac{\epsilon}{\tau\bar{\epsilon}}$. But $\left|\frac{\epsilon}{\tau\bar{\epsilon}}\right| = \left|1 + \frac{2b}{\tau(a - b\sqrt{2})}\sqrt{2}\right|$ and $\left|\frac{\bar{\epsilon}}{\tau\epsilon}\right| = \left|1 - \frac{2b}{\tau(a - b\sqrt{2})}\sqrt{2}\right|$ and we have also proved that $\tau(a - b\sqrt{2}) > 0$, hence $\left|\frac{\epsilon}{\tau\bar{\epsilon}}\right| > 1$ and $\left|\frac{\bar{\epsilon}}{\tau\epsilon}\right| < 1$. Then the $\max\left(1, \left|\frac{\epsilon}{\tau\bar{\epsilon}}\right|\right) = \left|\frac{\epsilon}{\tau\bar{\epsilon}}\right|$ and the $\max\left(1, \left|\frac{\bar{\epsilon}}{\tau\epsilon}\right|\right) = 1$, hence the logarithmic height of $\frac{\epsilon}{\tau\bar{\epsilon}}$ is given by

$$\begin{aligned}h\left(\frac{\epsilon}{\tau\bar{\epsilon}}\right) &= \frac{1}{2}\log\left(\epsilon\bar{\epsilon}\left|\frac{\epsilon}{\tau\bar{\epsilon}}\right|\right) \\ &= \frac{1}{2}\log\epsilon^2 \\ &= \log\epsilon.\end{aligned}$$

Since $\frac{\epsilon}{\tau\bar{\epsilon}} \in \mathbb{Q}\left[\sqrt{2}\right]$ but $\frac{\epsilon}{\tau\bar{\epsilon}} \notin \mathbb{Z}$ and $\frac{\epsilon}{\tau\bar{\epsilon}}$ is a root of the polynomial $f(X) = \epsilon\bar{\epsilon}X^2 - \tau\left(\epsilon^2 + \bar{\epsilon}^2\right)X + \epsilon\bar{\epsilon}$ with coefficients in $\mathbb{Z}$, then the polynomial $f(X) = \epsilon\bar{\epsilon}X^2 - \tau\left(\epsilon^2 + \bar{\epsilon}^2\right)X + \epsilon\bar{\epsilon}$ is the minimal polynomial of $\frac{\epsilon}{\tau\bar{\epsilon}}$ over $\mathbb{Z}$.

We are now considering ρ^2. For $\rho^2 = 3 + 2\sqrt{2}$ there are also two automorphisms in $\mathbb{Z}\left[\sqrt{2}\right]$ i.e the identity and $\sigma : 3 + 2\sqrt{2} \rightarrow 3 - 2\sqrt{2}$. Then $\left(X - (3 + 2\sqrt{2})\right)\left(X - (3 - 2\sqrt{2})\right) = 0$. Then the minimal polynomial of $3 + 2\sqrt{2}$ over $\mathbb{Q}$ is $g(X) = X^2 - 6X + 1$. The

$\max\left(1, 3+2\sqrt{2}\right) = 3+2\sqrt{2}$ and the $\max\left(1, 3-2\sqrt{2}\right) = 1$, then the logarithmic height of $3+2\sqrt{2}$ is given by

$$\begin{aligned} h\left(3+2\sqrt{2}\right) &= \frac{1}{2}\log\left(3+2\sqrt{2}\right) \\ &= \frac{1}{2}\log\left(1+\sqrt{2}\right)^2 \\ &= \log\left(1+\sqrt{2}\right). \end{aligned}$$

We also claim that $\frac{\epsilon}{\tau\bar{\epsilon}}$ and ρ^2 are multiplicatively independent algebraic numbers and $\frac{\epsilon}{\tau\bar{\epsilon}}$ is not a unit in $\mathbb{Z}[\sqrt{2}]$.

Proof

The monic minimal polynomial of $\frac{\epsilon}{\tau\bar{\epsilon}}$ over $\mathbb{Q}$ does not have integer coefficients, so $\frac{\epsilon}{\tau\bar{\epsilon}}$ is not an algebraic integer. Suppose $\left(\frac{\epsilon}{\tau\bar{\epsilon}}\right)^M = \rho^N$ for some $M, N \in \mathbb{Z}$. Taking reciprocals if necessary, we may assume that $M \geq 0$. Then since ρ^N is an algebraic integer, $\left(\frac{\epsilon}{\tau\bar{\epsilon}}\right)^M$ is also. Hence $\left(\left(\frac{\epsilon}{\tau\bar{\epsilon}}\right)^M\right)^r + a_1\left(\left(\frac{\epsilon}{\tau\bar{\epsilon}}\right)^M\right)^{r-1} + \cdots + a_r = 0$ for all $a_i \in \mathbb{Z}$. Unless $M = 0$, this contradicts the fact that $\frac{\epsilon}{\tau\bar{\epsilon}}$ is not an algebraic integer. If $M = 0$ then $\rho^N = 1$ and $N = 0$ as well, otherwise $\left(\frac{\epsilon}{\tau\bar{\epsilon}}\right)^M \neq \rho^N$ for $M \geq 1$. Then by Definition 4.10 $\frac{\epsilon}{\tau\bar{\epsilon}}$ and ρ are multiplicatively independent, so are ρ^2 and $\frac{\epsilon}{\tau\bar{\epsilon}}$.

We have $\{\rho^N\}$, a set of units in $\mathbb{Z}[\sqrt{2}]$ for $N \in \mathbb{Z}$, $\frac{\epsilon}{\tau\bar{\epsilon}} \neq \rho^N$ for all N and we have shown that $\frac{\epsilon}{\tau\bar{\epsilon}} > 1$, then $\frac{\epsilon}{\tau\bar{\epsilon}}$ is not a unit in $\mathbb{Z}[\sqrt{2}]$. ■

This concludes the elementary analysis of the equation (4.1).

STEP 2: We calculate an upper bound for m valid for the solutions of the equation (4.1).

From the equation (4.20) using Proposition 4.11 we have the following parameters:

$$\alpha_1 = \frac{\epsilon}{\tau\bar{\epsilon}},\ \alpha_2 = \rho^2 = 3+2\sqrt{2},\ b_1 = n,\ b_2 = t,\ p = 2,$$

$$\log A_1 = \log\epsilon,\ \log A_2 = \log(1+\sqrt{2}),\ b' = \frac{n}{2\log(1+\sqrt{2})} + \frac{t}{2\log\epsilon}.$$

Before we apply Proposition 4.11, let us check whether the conditions necessary for its application are satisfied by these parameters and show that $D = 2$ and $f = 1$.
From STEP 1 we have n and t positive integers and we have proved that for $\epsilon = a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$ and $a, b > 0$, a is odd, hence $A_1 > 1$ and $A_2 = 1 + \sqrt{2} > 1$. For $\alpha_1 = \frac{\epsilon}{\tau\bar{\epsilon}}$ and $\alpha_2 = \rho^2 = 3 + 2\sqrt{2}$, since a is odd then $\nu_2(\epsilon) = \nu_2(\bar{\epsilon}) = 0$ and by Lemma 3.3 $\nu_2(\alpha_1) = \nu_2(\alpha_2) = 0$ and hence by Definition 3.25 α_1 and α_2 are units in $\mathbb{Z}_2$, hence 2-adic units. We have already proved that α_1 and α_2 are multiplicatively independent. We can then conclude that these parameters satisfy the conditions necessary for the application of Propositions 4.11 and 4.12.

We have $K = \mathbb{Q}\left[\sqrt{2}\right]$, hence $[K : \mathbb{Q}] = 2$. Let $e = e\left(K/\mathbb{Q}\right)$ be the ramification index of K over $\mathbb{Q}$. Since $[K : \mathbb{Q}] = 2$ and the integer divisors of 2 are either 1 and 2, then either $e = 1$ or $e = 2$. Since $\alpha_1 \in K$ has a conjugate α_2 which is in K, this implies that the degree of the minimal polynomial of α_1 and α_2 is 2 and hence $e = 2$. Then we have $f = 1$, since $f = \frac{n}{e}$. By Definition 3.36 (2) this implies that $K/\mathbb{Q}$ is totally ramified. Since from Proposition 1 we have $D = \left[\mathbb{Q}\left(\alpha_1; \alpha_2\right)\right]/f$, then $D = 2$.

In order to bound m, we can apply Proposition 4.11 using the above parameters as they satisfy the necessary conditions for its application. From equation (4.20) we have $\nu_2(A_u) = \frac{m+2}{2}$. Then applying Proposition 4.11 yields

$$\begin{aligned} \frac{m+2}{2} &\leq \frac{18 \cdot 2(2-1)}{(\log 2)^4} \cdot 2^4 \max\left\{\log b' + \log\log 2 + 0.4, 10\right\}^2 \cdot \log\epsilon \cdot \log(1+\sqrt{2}) \\ m+2 &\leq 4400 \max\{\log b' + 0,034, 10\}^2 \log\epsilon. \end{aligned} \tag{4.21}$$

Dividing equation (4.18) by $\epsilon^n \rho^{-t}$ and letting the quotient be equal to Λ_a, we obtain

$$\frac{2^{(m+1)/2}\sqrt{2}}{\epsilon^n \rho^{-t}} = \frac{2^{(m+1)/2}\sqrt{2}}{x + 2^{(m-1)/2}\sqrt{2}} = 1 - \left(\frac{\bar{\epsilon}}{\tau\epsilon}\right)^n \rho^{2t} = \Lambda_a. \tag{4.22}$$

Then

$$\log\Lambda_a = \frac{m+2}{2}\log 2 + t\log\rho - n\log\epsilon. \tag{4.23}$$

We now consider the cases $\Lambda_a \geq \frac{1}{2}$ and $\Lambda_a < \frac{1}{2}$. For these two cases we show that $\log 2 + 1525 \max\{\log b' + 0.034, 10\}^2 \log \epsilon + 349 \max\{\log b' + 0.18, 10\}^2 \log \epsilon$ is an upper bound for $n \log \epsilon - t \log \rho$.

Proof

If $\Lambda_a \geq \frac{1}{2}$, then from equation (4.22) we have $\frac{2^{(m+1)/2}\sqrt{2}}{\epsilon^n \rho^{-t}} \geq \frac{1}{2}$ and hence $2^{(m+3)/2}\sqrt{2} \geq \epsilon^n \rho^{-t}$. Introducing logs to this inequality and using equation (4.21) yields

$$\begin{aligned} 2n \log \epsilon - 2t \log \rho &\leq (m+4) \log 2 \\ n \log \epsilon - t \log \rho &= \frac{m+2}{2} \log 2 + \log 2 \\ &\leq 1525 \max\{\log b' + 0.034, 10\}^2 \log \epsilon + \log 2. \end{aligned} \tag{4.24}$$

If $\Lambda_a < \frac{1}{2}$, for this case we claim that for $0 < \Lambda_a < \frac{1}{2} \Rightarrow \log |(1 - \Lambda_a)| \leq 2\Lambda_a$.

Proof

Let $x = 1 - \Lambda_a$, then $\frac{1}{2} < x < 1 \Rightarrow |\log x| \leq 2(1 - x)$. Now if $\frac{1}{2} < x < 1 \Rightarrow -\infty < \log x < 0$. So we must show that if $\frac{1}{2} < x < 1 \Rightarrow -\log x \leq 2(1 - x)$ and this implies that we have to show that $\log x + 2 - 2x > 0$. Set $f(x) = \log x + 2 - 2x$. We have $x = 0$ as the vertical asymptote of f and $f'(x) = \frac{1}{x} - 2$. If $f'(x) = 0$, then $x = \frac{1}{2}$ and hence the co-ordinate of the turning point of f is $\left(\frac{1}{2}, 0.307\right)$.

Sketching the graph of f using Mathematica yields:

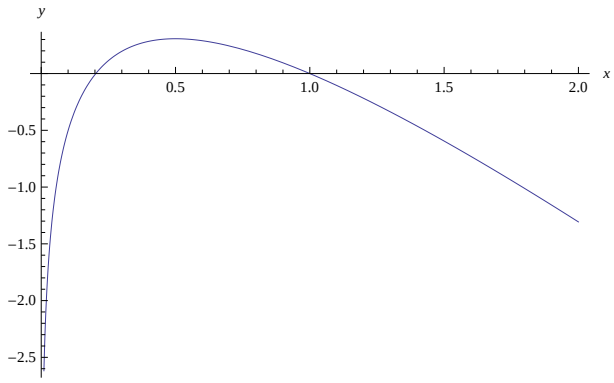

Figure 4.1: Graph of f.

From the graph of f we see that $f(x) > 0$ for $0.2 < x \leq \frac{1}{2}$ and $\frac{1}{2} < x < 1$. This proves

the claim.

From equation (4.22) we have $1-\Lambda_a = \left(\frac{\overline{\epsilon}}{\tau\epsilon}\right)^n \cdot \rho^{2t}$, then taking logs on both sides of this equation yields

$$\begin{aligned} |\log(1-\Lambda_a)| &= \left|\log\left(\left(\frac{\overline{\epsilon}}{\tau\epsilon}\right)^n \cdot \rho^{2t}\right)\right| \\ &= \left|t\log(3+2\sqrt{2}) - n\log\left(\frac{\tau\epsilon}{\overline{\epsilon}}\right)\right| \\ &= \left|n\log\left(\frac{\tau\epsilon}{\overline{\epsilon}}\right) - t\log(3+2\sqrt{2})\right|. \end{aligned} \tag{4.25}$$

From equation (4.25), we have the following parameters

$$\alpha_1 = \frac{\tau\epsilon}{\overline{\epsilon}},\ \alpha_2 = \rho^2 = 3+2\sqrt{2},\ b_1 = n,\ b_2 = t,\ D = 2,$$

$$\log A_1 = \log\epsilon, \quad \log A_2 = \log(1+\sqrt{2}) \text{ and } \quad b' = \frac{n}{2\log(1+\sqrt{2})} + \frac{t}{2\log\epsilon}.$$

We have already checked that these parameters satisfy the conditions necessary for the application of Proposition 4.12. Then the application of Proposition 4.12 yields

$$\log(|\log(1-\Lambda_a)|) \geq -24.7\cdot 2^4 \max\{\log b' + 0.18, 0.5, 10\}^2 \log\epsilon \cdot \log(1+\sqrt{2}) \tag{4.26}$$

$$\log 2\Lambda_a \geq -349\max\{\log b' + 0.18, 10\}^2 \log\epsilon \tag{4.27}$$

$$\log 2 + \log\Lambda_a \geq -349\max\{\log b' + 0.18, 10\}^2 \log\epsilon. \tag{4.28}$$

From the equations (4.23), (4.24) and (4.28) we infer that

$$\begin{aligned} n\log\epsilon - t\log\rho \leq \log 2 &+ 1525\max\{\log b' + 0.034, 10\}^2 \log\epsilon \\ &+ 349\max\{\log b' + 0.18, 10\}^2 \log\epsilon \end{aligned}$$

holds. ■

STEP 3: We calculate an upper bound for n valid for the solutions of the equation (4.1) and show that $0 < n \leq 5.5\times 10^5$ for all the solutions of the equation (4.1).

From equation (4.1) we have $x^2 = y^n + 2^m$ and hence $x^2 > y^n \Rightarrow x > y^{\frac{n}{2}}$ and from equation (4.17) we have $x + 2^{\frac{m-1}{2}}\sqrt{2} = \epsilon^n\rho^{-t} \Rightarrow \epsilon^n\rho^{-t} > x$ and hence $\epsilon^n\rho^{-t} \geq y^{\frac{n}{2}}$. After introducing

logs on both sides of the inequality $\epsilon^n \rho^{-t} \geq y^{\frac{n}{2}}$, we have $n \log \epsilon - t \log \rho \geq \frac{n}{2} \log y$. Substituting in equation (4.29) $n \log \epsilon - t \log \rho$ by $\frac{n}{2} \log y$ and then solve for n yields

$$n \leq \frac{2 \log 2}{\log y} + 3050 \max\{\log b' + 0.18, 10\}^2 \frac{\log \epsilon}{\log y} + 698 \max\{\log b' + 0.034, 10\}^2 \frac{\log \epsilon}{\log y}. \tag{4.29}$$

We note that $\log y \neq 0$ since from the hypothesis $y > 1$.

In order to get a better bound for n, we will consider two cases, when $\epsilon < 8$ and $\epsilon > 8$ separately.

For $\epsilon < 8$, we let $\mathcal{E} = \{1 + 2\sqrt{2}, 1 + 3\sqrt{2}, 1 + 4\sqrt{2}, 1 + 5\sqrt{2}, 3 + \sqrt{2}, 5 + \sqrt{2}, 5 + 2\sqrt{2}\}$, the set of $\epsilon = a + b\sqrt{2}$ with co-prime positive integers a and b such that a is odd and ϵ is not the set of units in $\mathbb{Z}\left[\sqrt{2}\right]$.

Let us now bound n for each $\epsilon \in \mathcal{E}$ using the equation (4.29). We have to note that y is positive.

1. If $\epsilon = 1 + 2\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 7$, $\dfrac{\log \epsilon}{\log y} = \dfrac{\log(1 + 2\sqrt{2})}{\log 7} = 0.4529$, $b' \leq 0.9397n$ and

$$\begin{aligned} n &\leq 0.7124 + 1381.345 \left(\log n - 0.028\right)^2 + 316.12 \left(\log n + 0.118\right)^2 \\ n &\leq 1697.47 \left(\log n\right)^2 - 2.751 \log n + 6. \end{aligned}$$

2. If $\epsilon = 1 + 3\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 17$, $\dfrac{\log \epsilon}{\log y} = \dfrac{\log(1 + 3\sqrt{2})}{\log 17} = 0.5848$, $b' \leq 0.86908n$ and

$$\begin{aligned} n &\leq 0.4893 + 1783.64 \left(\log n - 0.106\right)^2 + 408.1904 \left(\log n + 0.04\right)^2 \\ n &\leq 2191.8 \left(\log n\right)^2 - 345.47 \log n + 21.183. \end{aligned}$$

3. If $\epsilon = 1 + 4\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 31$, $\dfrac{\log \epsilon}{\log y} = \dfrac{\log(1 + 4\sqrt{2})}{\log 31} = 0.55202$, $b' \leq 0.83106n$ and

$$\begin{aligned} n &\leq 0.4037 + 1683.6 \left(\log n - 0.151\right)^2 + 385 \left(\log n - 0.006\right)^2 \\ n &\leq 2068.6 \left(\log n\right)^2 - 513.067 \log n + 38.805. \end{aligned}$$

4. If $\epsilon = 1 + 5\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 49$, $\dfrac{\log \epsilon}{\log y} = \dfrac{\log(1 + 5\sqrt{2})}{\log 49} = 0.5366$, $b' \leq 0.8067n$ and

$$\begin{aligned} n &\leq 0.3562 + 1636 \left(\log n - 0.181\right)^2 + 374.5468 \left(\log n - 0.035\right)^2 \\ n &\leq 2010.55 \left(\log n\right)^2 - 618.45 \log n + 54.412. \end{aligned}$$

5. If $\epsilon = 3+\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 7$, $\dfrac{\log\epsilon}{\log y} = \dfrac{\log(3+\sqrt{2})}{\log 7} = 0.76305$, $b' \leq 0.90404n$ and

$$\begin{aligned} n &\leq 0.7124 + 2327.3025\,(\log n - 0.067)^2 + 532.6089\,(\log n - 0.079)^2 \\ n &\leq 2859.91\,(\log n)^2 - 396.011\log n + 14.484. \end{aligned}$$

6. If $\epsilon = 5+\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 23$, $\dfrac{\log\epsilon}{\log y} = \dfrac{\log(1+2\sqrt{2})}{\log 23} = 0.5927$, $b' \leq 0.8363n$ and

$$\begin{aligned} n &\leq 0.4421 + 1807.735\,(\log n - 0.145)^2 + 413.7046\,(\log n + 0.001)^2 \\ n &\leq 2221.44\,(\log n)^2 - 523.416\log n + 38.45. \end{aligned}$$

7. If $\epsilon = 5+2\sqrt{2}$, then $y = \tau\bar{\epsilon}\epsilon = 17$, $\dfrac{\log\epsilon}{\log y} = \dfrac{\log(5+2\sqrt{2})}{\log 17} = 0.77$, $b' \leq 0.81n$ and

$$\begin{aligned} n &\leq 0.50 + 2348\,(\log n - 0.17)^2 + 357\,(\log n - 0.033)^2 \\ n &\leq 2705\,(\log n)^2 - 821.882\log n + 68.746. \end{aligned}$$

Let us now calculate an upper bound for n when $\epsilon > 8$ using equation (4.29). From STEP 1 we have $0 < t \leq n$, then on the LHS of equation (4.29) we substitute t by n and take $\log\epsilon$ as a common factor and this yields

$$n\log\epsilon - t\log\rho \geq n\left(1 - \frac{\log\rho}{\log\epsilon}\right)\log\epsilon.$$

Let us consider $\epsilon \geq 7+\sqrt{2}$. Then for $\epsilon = 7+\sqrt{2}$ and $\rho = 1+\sqrt{2}$ we have $\left(1 - \dfrac{\log\rho}{\log\varepsilon}\right)^{-1} \leq 1.71$ and $b' \leq 0.81n$. To solve for n in equation (4.29) we multiply equation (4.29) by $\dfrac{1.71}{\log\epsilon} \leq \dfrac{1.71}{\log(7+\sqrt{2})}$ and substitute b' by $0.81n$ and that yields

$$n \leq 0.56 + 2608\max\{\log n - 0.17, 10\}^2 + 597\max\{\log n - 0.033, 10\}^2. \qquad (4.30)$$

We observe that for $\epsilon < 8$ the upper bounds for n lie below that in (4.30) and hence we may conclude that $0.56 + 2608\max\{\log n - 0.17, 10\}^2 + 597\max\{\log n - 0.033, 10\}^2$ is an upper bound for n.

In equation (4.30) we assume that $\log n - 0.17 > 10$ and $\log n - 0.033 > 10$. If $\log n - 0.17 > 10$, then $n > 26108.08$ and this satisfies both of our assumptions. Now we have

$$\begin{aligned} n &\leq 0.56 + 2608\{\log n - 0.17\}^2 + 597\{\log n - 0.033\}^2 \\ &\leq 3205\left(\log n\right)^2 - 922,54\left(\log n\right) + 76.47. \end{aligned} \tag{4.31}$$

Reducing the inequality in equation (4.31) by dividing by n yields

$$1 \leq 3205\frac{\left(\log n\right)^2}{n} - 922.54\left(\frac{\log n}{n}\right) + \frac{76.47}{n}. \tag{4.32}$$

Now we want to find the value(s) of n satisfying the inequality in equation (4.32).
Let $n = x$, $f\left(x\right) = 3205\frac{\left(\log x\right)^2}{x} - 922.54\left(\frac{\log x}{x}\right) + \frac{76.47}{x}$ and $g\left(x\right) = 1$.

We now calculate the features of the graph of f.
y-intercept and vertical asymptote: There is no y-intercept since $\log x$ is undefined when $x = 0$ and hence $x = 0$ is a vertical asymptote of f.

horizontal asymptote: Since $\lim\limits_{x\to\infty}\left(\frac{\left(\log x\right)^2}{x}\right) = 0$, $\lim\limits_{x\to\infty}\left(\frac{\left(\log x\right)}{x}\right) = 0$ and $\lim\limits_{x\to\infty}\left(\frac{1}{x}\right) = 0$, then $\lim\limits_{x\to\infty} f\left(x\right) = 0$ and hence $y = 0$ is the horizontal asymptote of f.

x-intercepts: If $f\left(x\right) = 0$, cross multiplying by x yields $3205\left(\log x\right)^2 - 922,54\left(\log x\right) + 76.47 = 0$ and the discriminant for this equation is -129265.34 and hence this equation has no solution in $\mathbb{R}$ and hence f has no x-intercepts in $\mathbb{R}$.

$$f'\left(x\right) = \frac{-3205\left(\log x\right)^2 + 7332.54\left(\log x\right) - 999.01}{x^2} \tag{4.33}$$

turning points: If $f'\left(x\right) = 0$, then from equation (4.33) we get $\log x = 0.145$ or $\log x = 2.142$ and hence $x = 1.156$ or $x = 8.516$. Then the co-ordinates of the turning points of f are $(1.156, 8.726)$ and $(8.516, 1503.694)$.

$$f''\left(x\right) = \frac{6410\left(\log x\right)^2 - 21075.08\left(\log x\right) + 9330.56}{x^3} \tag{4.34}$$

points of inflection: If $f''(x) = 0$, then from equation (4.34) we get $\log x = 0.527$ or $\log x = 2.761$ and hence $x = 1.694$ or $x = 15.816$. Then the co-ordinates of the points of inflection of f are $(1.694, 283.597)$ and $(15.816, 1388.558)$.

From equation (4.34) we have $f''(1.156) = 4149.149 > 0$ and $f''(8.516) = -10.366 < 0$ and hence $(1.156, 8.726)$ is the minimum turning point and $(8.516, 1503.694)$ is the maximum turning point of f.
Sketching the graph of f using Mathematica yields:

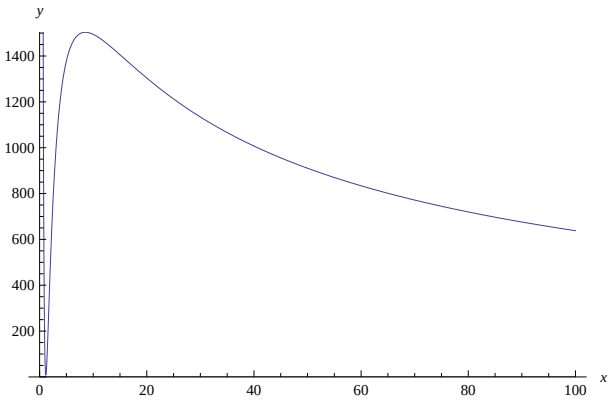

Figure 4.2: Graph of f.

Since $\log x > 10.17$, we have found through substitution that if $\log x > 13.21$, i.e $x > 545795.69$, then $f(x) > g(x)$. Hence any solution of the equation (4.1) has $0 < n \leq 545795$.

CONCLUSION: We prove that the equation (4.1) has finitely many solutions.
Since we are interested in proving that the equation (4.1) has finitely many solutions, we may assume that x, y, m and n are very large. We have proved that if (x, y, m, n) is a solution of the equation (4.1), then x, y, m and n are odd and from the hypothesis we have $y > 1$ and $n > 2$, hence the $\min(x, y, m, n) \geq 3$. We have also proved that $0 < n \leq 545795$, hence n is bounded.

From the equation (4.1) we have $x^2 - y^n = 2^m$, hence $P[x^2 - y^n] = 2$ and we have

$|x| > |y|^{\frac{n}{2}}$ for all $3 \leq n \leq 545795$. Let X and c_1 be effectively computable constants depending on n such that $\max(|x|, |y|) = X$, hence $3 \leq X$. Then by applying Lemma 4.7 we have $P[x^2 - y^n] = 2 \geq c_1 (\log\log X \log\log\log X)^{1/2}$, hence

$$\left| c_1 (\log\log X \log\log\log X)^{1/2} \right| \leq 2. \tag{4.35}$$

This implies that 2 is the upper bound of $c_1 (\log\log X \log\log\log X)^{1/2}$. If there are infinitely many solutions x and y of the equation $x^2 - y^n = 2^m$, then we can take $X \to \infty$ since we have assumed that x and y are very large and hence $c_1 (\log\log X \log\log\log X)^{1/2} \to \infty$ and this contradicts the inequality in equation (4.35). Hence there are finitely many values of X satisfying the inequality in equation (4.35) such that $3 \leq n \leq 545795$ and hence the equation (4.1) has finitely many solutions.

■

References

[1] Y. Bugeaund, On the Diophantine Equation $x^2 - 2^m = \pm y^n$, Proc.Amer.Math Soc 125 (1997), 3203 - 3208.

[2] Y. Bugeaund and M. Laurent, Minoration effective de la distance p-adique entre puissance de nombres, J. Number Th.61 (1996), 311 - 342.

[3] Minking Eie, Topics in Number Theory, world Scientific Publication, Co Ptc Ltd, 2009.

[4] John B. Fraleigh, A First Course in Abstract Algebra, Addison Wesley longman, 2000.

[5] A. Gica, The Diophantine equation $y^2 = 5^x + 11^x$, Rev. Roumaine Math. Pure Appl. , 49 (2004), 5 - 6, 455 - 459.

[6] A. Gica and L. Panaitopol, On Obláth's problem, J Integer Sequences 6 (2003).

[7] Y. Guo and G. Le, A note on the Diophantine equation $x^2 - 2^m = y^n$, Proc.Amer.Math Soc 123 (1995), 3627 - 3629 MR 962b:11040.

[8] Fernado Q. Gouvêa, p-adic Numbers, Springer-Verlag, Berlin Heidelberg, USA, 1993.

[9] S. Hyyrö, Ueber das Catalansche Problem Ann. Uni. Turky Ser Al, 79 (1964), 3 - 10 MR 31:3378.

[10] Gareth A. Jones and J. Mary Jones, Elementary Number Theory, Springer-Verlag, Berlin Heidelberg, London, 1998.

[11] Neal Koblitz, p-adic Numbers, p-adic Analysis and Zeta Functions, Springer-Verlag, Berlin Heidelberg, NY, 1977.

[12] S.V. Kotov, Ueber die maximale Norm der Idealteiler des polynoms $\alpha x^m + \beta y^n$ mit den algebraischem koeffizeinten, Acta Arith. 31 (1976), 219 - 230 MR 55:261.

[13] M. Laurent, M. Mignotte and Y. Nesterenko, Formes linéaires en deux logarithmes et detérminants d'interpolation, J. Number Th.55 (1995), 285 - 321. MR196h:11075.

[14] R.A. Mollin, Advanced Number Theory with Applications, CRS Press, 2009.

[15] L.J. Mordell, Diophantine Equations, Academy Press, London, 1969.

[16] Planetmath.org.

[17] Alian Robert, A course in p-adic Analysis,Springer-Verlag, Berlin Heidelberg, NY, 2000.

[18] T.N. Shorey and R. Tijdeman, Exponential Diophantine Equations, Cambridge University Press, NY, 1986.

[19] Michel Waldschmidt, Diophantine Approximation on Linear Algebraic Groups, Springer-Verlag, Berlin Heidelberg, Germany, 2000.

[20] Wikipedia.

[21] Kenneth S. Williams, Introductory Algebraic Number Theory, Cambridge University Press, USA, 2004.